

BANK OF RUSSIA STANDARD

STO BR BFBO-1.5-2018

SECURITY OF FINANCIAL (BANKING) OPERATIONS INFORMATION SECURITY INCIDENT MANAGEMENT

ON THE FORMS AND TIMEFRAMES OF THE BANK OF RUSSIA'S INTERACTION WITH INFORMATION EXCHANGE PARTICIPANTS IN THE EVENT OF DETECTION OF INCIDENTS RELATED TO VIOLATIONS OF DATA PROTECTION REQUIREMENTS

Effective date: 1 November 2018

Official edition

Moscow 2018

Preface

APPROVED AND IMPLEMENTED by Bank of Russia Order No. OD-2403, dated 14 September 2018. This Standard shall not be reproduced, replicated or distributed, whether in full or in part, as an official edition, unless authorised by the Bank of Russia.

Contents

| Int | troduction4 |
|-----|---|
| 1. | Scope |
| 2. | Regulatory references |
| 3. | Terms and definitions |
| 4. | Designations and abbreviations12 |
| | The data submission form used by information exchange participants for registration with the Bank of Russia |
| | Data submission form used by information exchange participants to inform the Bank of Russia about incidents related to violations of data protection requirements and the timeframes for their submission to the Bank of Russia |
| | The form of the Bank of Russia's request to the information exchange participant serving the payee |
| | The data submission form used by information exchange participants to provide a response to the Bank of Russia's request to the information exchange participant servicing the payee and the timeframes for their submission to the Bank of Russia |
| | The form of information message of the Bank of Russia to the information exchange participant serving the payer |
| | b. The form for submitting a request to the Bank of Russia from information request participants who are not structural units of the Bank of Russia using the express and non-rapid money transfer platforms, about imposing (or lifting) restrictions on their bank (correspondent) accounts (sub-accounts) in the form of a ban to debit funds upon detecting incidents related to violations of data protection requirements during money transfer |
| | . The form of an information message of the Bank of Russia on imposing (or lifting) the restriction on the bank (correspondent) accounts (sub-accounts) of information exchange participants in the form of a ban to debit fundscpeдств |
| | 2. The form of distribution by the Bank of Russia among information exchange participants of data on the detected incidents associated with violations of data protection requirements |
| | 8. The form of data submission used by information exchange participants to send information to the Bank of Russia on planned measures to disclose information on identified incidents related to violations of data protection requirements and timeframes for their submission to the Bank of Russia |
| | Conditions for information exchange participants to submit to the Bank of Russia |
| | data on detected incidents related to a violation of data protection requirements |
| | |
| | b. Description of the technology for preparing and sending electronic messages during information exchange with the Bank of Russia |

| Annex 1. Schemes of interaction between an information exchange participant and the Bank of Russia |
|--|
| Annex 2. Schemes of interaction between the Bank of Russia and an information exchange participant |
| Annex 3. Diagrams of processes of interaction between an information exchange participant and the Bank of Russia |
| Bibliography |

Introduction

This standard defines the following aspects of the Bank of Russia's interaction with credit institutions, non-bank financial institutions, and entities of the national payment system (hereinafter, information exchange participants) when incidents related to violation of data protection requirements are detected:

- the data submission form used by information exchange participants for registration with the Bank of Russia;
- the data submission form used by information exchange participants to inform the Bank of Russia about incidents related to violations of data protection requirements and the timeframes for their submission to the Bank of Russia;
- the form of the Bank of Russia's request to the information exchange participant serving the payee;
- the data submission form used by information exchange participants to provide a response to the Bank of Russia's request to the information exchange participant servicing the payee and the timeframes for their submission to the Bank of Russia;
- the form of information message of the Bank of Russia to the information exchange participant serving the payer;
- the data submission form used by information exchange participants to submit a request to the Bank of Russia to impose (or lift) a restriction on their bank (correspondent) accounts (subaccounts) in the form of a ban on debiting funds upon detecting incidents related to violation of data protection requirements;
- the form of a Bank of Russia information message on imposing or lifting restrictions in the form of a ban on debiting funds on bank (correspondent) accounts (sub-accounts) of information exchange participants upon detecting incidents related to violation of data protection requirements;
- the form of distribution by the Bank of Russia to information exchange participants of data on detected incidents related to violation of data protection requirements;
- the form of data submission used by information exchange participants to send information to the Bank of Russia on planned measures to disclose information on identified incidents related to violation of data protection requirements and the timeframes for their submission to the Bank of Russia;
- conditions for information exchange participants to submit to the Bank of Russia data on identified incidents related to violation of data protection requirements;
- description of the technology for preparing and sending electronic messages during information exchange with the Bank of Russia.

The data submission form used by information exchange participants to inform the Bank of Russia about incidents related to violations of data protection requirements shall be used in the following cases:

 when money transfer operators and payment infrastructure service providers inform the Bank of Russia about the detected incidents related to the violation of data protection requirements when making money transfers, in accordance with the Bank of Russia's requirements [3];

- when money transfer operators and payment infrastructure service providers inform the Bank of Russia about all cases and (or) attempts to make money transfers without the customer's consent in accordance with the requirements of the Bank of Russia [4];
- when credit institutions inform the Bank of Russia about the revealed incidents related to the violation of the requirements for ensuring information protection in the course of banking activities, in accordance with the requirements of the Bank of Russia [5];
- when non-bank financial institutions inform the Bank of Russia about the detected incidents related to the violation of the requirements for ensuring the protection of information in the course of activities in financial markets, in accordance with the requirements of the Bank of Russia [6];
- when money transfer operators inform the Bank of Russia about the suspension of funds crediting to the payee's bank account or the increase in the balance of the payee's electronic funds in accordance with the Bank of Russia's requirements [20];

The form of the Bank of Russia's request to an information exchange participant serving the payee shall apply:

- when requesting from the money transfer operator servicing the payee, including the emoney operator, information identifying the payee, in accordance with the requirements of the Bank of Russia [4];
- when sending a notice of suspension of the transfer of funds to the payee's bank account or an increase in the balance of the payee's electronic funds in accordance with the requirements of the Bank of Russia [20].
- The data submission form used by information exchange participants to provide a response to the Bank of Russia's request to an information exchange participant serving the payee shall be used:
- when the money transfer operator serving the payee, including the electronic funds operator, informs the Bank of Russia about a specific payee in accordance with the requirements of the Bank of Russia [4];
- when sending a notification about the successful suspension of the money transfer to the bank account of the payee or an increase in the balance of the payee's electronic funds in accordance with the requirements of the Bank of Russia [20];
- when sending a notification about the impossibility to suspend the money transfer to the payee's bank account or increasing the balance of the payee's electronic funds in accordance with the requirements of the Bank of Russia [20].

The form of the Bank of Russia's information message to an information exchange participant serving the payer shall be used:

- when sending a notification about the successful suspension of the money transfer to the bank account of the payee or an increase in the balance of the payee's electronic funds in accordance with the requirements of the Bank of Russia [20];
- when sending a notification about the impossibility to suspend the money transfer to the payee's bank account or increasing the balance of the payee's electronic funds in accordance with the requirements of the Bank of Russia [20].

The data submission form used by information exchange participants to send a request to the Bank of Russia on imposing (or lifting) the restriction on their bank (correspondent) accounts (sub-accounts) in the form of a ban on debiting funds upon detecting incidents related to violation of data protection requirements shall apply as follows:

 when exchange participants using speedy and non-speedy money transfer services and which are not Bank of Russia structural units;

inform the Bank of Russia about imposing restrictions on their bank (correspondent) accounts (sub-accounts) in the form of a ban on debiting funds upon detecting incidents related to violations of data protection requirements during money transfers at the information infrastructure facilities of information exchange participants in accordance with requirements of the Bank of Russia [21];

- when exchange participants using the speedy and non-speedy money transfer services and which are not Bank of Russia structural units inform the Bank of Russia about lifting restrictions on their bank (correspondent) accounts (sub-accounts) in the form of a ban on debiting funds upon detecting incidents related to violations of data protection requirements during money transfers at the information infrastructure facilities of information exchange participants in accordance with requirements of the Bank of Russia [21].

The form of a Bank of Russia information notice about imposing or lifting a restriction on the bank (correspondent) accounts (sub-accounts) of information exchange participants in the form of a ban on debiting funds shall be used as follows:

- when sending a notification to an information exchange participant in case of achieving a
 positive result of integrity control and acceptance of requests for imposing or lifting
 restrictions in the form of a ban on debiting funds in accordance with the requirements
 of the Bank of Russia [21];
- when sending a notification to an information exchange participant in case of achieving a negative result of integrity control and non-acceptance for execution of requests for imposing or lifting restrictions in the form of a ban on debiting funds in accordance with the requirements of the Bank of Russia [21].

The form for distribution by the Bank of Russia of data on detected incidents related to violation of data protection requirements among information exchange participants shall be used when sending information contained in the database on cases and attempts to make money transfers without the customer's consent in accordance with the requirements of the Bank of Russia [4].

The data submission form for information exchange participants to send information to the Bank of Russia on planned measures for disclosing information on identified incidents related to violation of data protection requirements shall be used to inform the Bank of Russia by money transfer operators and payment infrastructure service providers about the above measures in accordance with the requirements of the Bank of Russia [3].

The data submission form for information exchange participants to send information to the Bank of Russia on planned measures for disclosing information on identified incidents related to violations of information protection requirements in the course of banking activities shall be used to inform the

Bank of Russia about the above-mentioned measures in accordance with the Bank of Russia's requirements [5].

The data submission form for information exchange participants to send information to the Bank of Russia on planned measures to disclose information on identified incidents related to violation of information protection requirements in the course of financial market activities shall be used to inform non-bank financial institutions of the above-mentioned measures in accordance with the Bank of Russia's requirements [6].

BANK OF RUSSIA STANDARD

SECURITY OF FINANCIAL (BANKING) OPERATIONS INFORMATION SECURITY INCIDENT MANAGEMENT

ON THE FORMS AND TIMEFRAMES OF THE BANK OF RUSSIA'S INTERACTION WITH INFORMATION EXCHANGE PARTICIPANTS IN THE EVENT OF INCIDENTS RELATED TO VIOLATIONS OF THE DATA PROTECTION REQUIREMENTS

Effective date: 1 November 2018

1. Scope

This standard establishes the form and timeframes for the Bank of Russia's interaction with information exchange participants to identify incidents related to violations of data protection requirements.

This standard is recommended for use by including references hereto and/or direct use of the provisions hereof in the internal documentation of information exchange participants, as well as in agreements.

The mandatory application of this standard by other organisations may be defined by an agreement on cooperation with the Bank of Russia on countering computer attacks.

2. Regulatory references

This standard shall refer to the following documents:

Federal Law No. 86-FZ, dated 10 July 2002, 'On the Central Bank of the Russian Federation (Bank of Russia)' [1];

Federal Law No. 161-FZ, dated 27 June 2011, 'On the National Payment System' [2];

Bank of Russia Regulation No. 382-P, dated 9 June 2012, 'On Requirements to Protect Information Related to Funds Transfers and on the Procedure for the Bank of Russia to Control the Compliance with Requirements to Protect Information Related to Funds Transfers' [3];

the Bank of Russia's regulation establishing the forms and procedure for sending information by money transfer operators, payment system operators and payment infrastructure service providers to the Bank of Russia on all cases and attempts to make money transfers without the customer's

consent and receiving information from the Bank of Russia, contained in the database on cases and attempts to make money transfers without the customer's consent, and the procedure for taking measures by money transfer operators, payment system operators, and payment infrastructure service providers to prevent money transfers without the customer's consent [4];

the Bank of Russia's regulation establishing mandatory requirements for credit institutions to ensure data protection in the course of banking activities [5];

the Bank of Russia's regulation establishing mandatory requirements for non-bank financial institutions to ensure data protection in financial markets [6];

the Bank of Russia's regulation establishing the forms and procedure for money transfer operators to send notifications about suspending money transfers to the payee's bank account or increasing the payee's electronic money balance, as well as about the impossibility of suspending money transfers to the bank account of the payee or suspending the increase in the electronic money balance of the payee [20];

the Bank of Russia's regulation establishing requirements for ensuring data protection in the Bank of Russia payment system [21].

3. Terms and definitions

This standard uses the terms defined in the following documents: Federal Law No. 161-FZ, dated 27 June 2011, 'On the National Payment System' [2]; Bank of Russia Regulation No. 382-P, dated 9 June 2012, 'On Requirements to Protect Information Related to Funds Transfers and on the Procedures for the Bank of Russia to Control the Compliance with Requirements to Protect Information Related to Funds Transfers' [3];

The Bank of Russia's regulation establishing the forms and procedure for money transfer operators, payment system operators, and payment infrastructure service providers to send information to the Bank of Russia on all cases and attempts to make money transfers without the customer's consent and for receiving information from the Bank of Russia contained in the database of cases and attempts to make money transfers without the customer's consent, and the procedure for money transfer operators, payment system operators, payment infrastructure service providers to take measures to prevent money transfers without the customer's consent [4];

The Bank of Russia's regulation establishing mandatory requirements for credit institutions to ensure data protection in the course of banking activities [5];

The Bank of Russia's regulation establishing mandatory requirements for non-bank financial institutions to ensure data protection in financial markets [6];

National Standard of the Russian Federation GOST R ISO/IEC 15 408-3-2013 'Information Technology. Security Methods and Tools. Criteria for Assessing Information Technology Security. Part 3. Security Confidence Components' [19];

The Bank of Russia's regulation establishing the forms and procedure for money transfer operators to send notifications about suspending money transfers to the payee's bank account or increasing the payee's electronic money balance, as well as about the impossibility of suspending money transfers to the bank account of the payee or suspending the increase in the electronic money balance of the payee [20];

The Bank of Russia's regulation establishing requirements for ensuring data protection in the Bank of Russia payment system [21].

- 3.1. Incidents associated with violations of data protection requirements include:
 - incidents associated with violations of data protection requirements when making money transfers;
 - incidents associated with violations of data protection requirements in the course of banking activities;
 - incidents associated with violations of data protection requirements in financial markets;
 - incidents associated with a failure to provide money transfer services or their untimely provision;
 - incidents associated with a failure to provide financial (banking) services or their untimely provision.

3.2. For the purposes of this standard, an incident involving a violation of data protection requirements shall mean one or a series of related undesirable or unexpected data protection events that may result or have already resulted in the following negative consequences:

- transferring funds without the customer's consent;
- conducting a financial (banking) operation without the customer's consent;
- a failure to provide money transfer services or their untimely provision;
- a failure to provide financial (banking) services or their untimely provision.
- Data protection shall include the following events:
- a) receiving notifications by information exchange participants, including:
- upon receiving by the money transfer operator servicing the payer, including the e-money operator, of notifications in the form provided for by the relevant contract from customers, including individuals, legal entities, individual entrepreneurs, or persons engaged in private businesses, about actual and (or) attempted money transfers without the customer's consent and the use of electronic payment instruments;
- when the money transfer operator servicing the payee, including the e-money operator, identifies transactions with signs of a money transfer without the customer's consent established by the Bank of Russia and posted on the Bank of Russia website;
- receiving by the payment system settlement centre of notifications from payment system participants about funds debiting from their correspondent accounts without their consent and (or) using distorted information contained in the orders of payment clearing centres or payment system participants;

• receiving notifications from individual customers, and (or) individual entrepreneurs, and (or) persons engaged in private businesses in accordance with the procedure established by Russian laws, and (or) legal entities on conducting financial (banking) operations without their consent;

b) the identified occurrence and (or) a change in the condition of an aggregate of access objects and resources, information processing facilities and systems, including automated systems (hereinafter, AS) used to provide IT support to business processes and (or) technological processes of information exchange participants, which may have the following consequences:

- identification by the money transfer operator servicing the payer, including the electronic money operator, of money transfer and cash receipt transactions resulted from unauthorised access to the information infrastructure of the money transfer operator, including when the balance of electronic funds, excluding virtual payment cards, is reduced;
- conducting financial (banking) operations as a result of unauthorised access to information infrastructure facilities of a non-bank financial institution;
- unauthorised withdrawal of funds of the money transfer operator at ATMs;
- unauthorised withdrawal of funds of the electronic money operator at ATMs;
- a failure to provide money transfer services or their untimely provision by the money transfer operator;
- a failure to provide by settlement services or their untimely provision by the settlement centre of an important payment system;
- a failure to provide payment clearing services or their untimely provision by the payment clearing centre of an important payment system;
- a failure to provide operational services or their untimely provision by the operational centre of an important payment system;
- a failure to provide financial (banking) services or their untimely provision;
- identification by the money transfer operator, including the electronic money operator and (or) the payment infrastructure service provider, of attacks which, if launched, may result in actual and attempted money transfers without the customer's consent.

4. Designations and abbreviations

DDoS (Distributed Denial of Service) is a distributed 'denial of service' attack with a simultaneous use of a large number of attacking computers as a rule aimed at partial disrupting of the nominal functionality of the information structure of an organisation

IPv4 – Internet Protocol version 4

URL - Uniform Resource Locator

AS – Automated system(s)

BIN – Bank Identification Number is a part of the payment card number used to identify the issuing bank within the card payment system during authorisation, processing and clearing operations

Botnet is a computer network consisting of nodes running the same type of centrally managed malware

MC – Malicious Code

MCSE - Malicious Code Side Effect(s)

CII - Critical Information Infrastructure

OGRN – Primary State Registration Number

OKOPF - All-Russian Classifier of Organisational and Legal Forms

OKTMO - All-Russian Classifier of Municipal Territories

OS – operating system

Internet – Internet Telecommunications Network

CIPF – Cryptographic Information Protection Facility

SNILS – individual insurance account number of the insured in the customised account system of the Pension Fund of the Russian Federation

5. The data submission form used by information exchange participants for registration with the Bank of Russia

5.1. Mandatory conditions and time characteristics of information provision

Mandatory information conditions:

[O] – information of the data block (field) shall be provided as required;

[N] [N] – information of the data block (field) shall be provided in the case of technical capability.

Time characteristics of information provision (stages of information provision):

[1] - information of the data block (field) shall be provided within the registration of an information exchange participant;

[2] - information of the data block (field) shall be provided as part of the change in registration data of an information exchange

participant.

5.2. Registration data of an information exchange participant. Data block [HEADER]

| | | | | · · · · | | |
|---------------------------------|--|---|---|---|-------------------------------|---------------------------------------|
| Data block (field) No. | ldentifier of data block (field) | Content of data block (field) | Data field format | E-mail format | Obligation of informing | Stages of information provision |
| 1.1 | ʻschemaType' (data field) | type of electronic message | Specify the value of [PARTICIPANT] – information exchange participant | { | [0] | [1], [2] |
| 1.2 | 'schemaVersion' (data field) | version of electronic message type scheme | Textarea (text field) | 'version': '1', 'memberld': '9527dd0c-0765-4f1c-8f5f- 70a02cf4046c', 'sourceld': 'f34030ef-358a-445c- 8567-25985ce6d91c', 'publishedAt': '2002-10- | [0] | [1], [2] |
| 1.3 | 'version' (data field) | version number of electronic message during information exchange | numeric value (int) | 02T15:00:00.05Z', 'modifiedAt': '2002-10- 02T15:00:00.05Z' }, | [0] | [1], [2] |
| 1.4 | ʻmemberld' (data field) | identifier of an information exchange participant assigned by the Bank of Russia | 128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by the Bank of Russia | | [0] | [2] |
| 1.5 | 'sourceld' | Identifier | 128-bit identifier | | [0] | [1], [2] |

| | (data field) | assigned by | (GUID) generated in |
|-----|---------------|----------------|--------------------------|
| | (uata field) | | |
| | | an | accordance with |
| | | information | Specification RFC 4122 |
| | | exchange | [16] assigned by an |
| | | participant | information exchange |
| | | | participant |
| 1.6 | 'publishedAt' | date and | data provision format in |
| | (data field) | time of | accordance with |
| | | registration | Specification RFC 3339 |
| | | of an | [11] |
| | | information | |
| | | exchange | |
| | | participant | |
| 1.7 | 'modifiedAt' | date and time | data provision format in |
| | (data field) | of a change in | accordance with |
| | | - | Specification RFC 3339 |
| | | registration | [11] |
| | | data of an | |
| | | information | |
| | | exchange | |
| | | participant | |

5.3. Registration data of an information exchange participant. Data Block [**PARTICIPANT**]

| Data block (field) No. | ldentifier of data block (field) | Content of data block (field) | Data field format | E-mail format | Obligation of informing | Stages of information provision |
|---------------------------------|-------------------------------------|--|---|-----------------------------|----------------------------|---------------------------------------|
| 2.1 | ʻorgld' (data field) | information exchange participant identifier | It is determined by the type of an information exchange participant: • an information exchange participant operating as a money transfer operator – the number of the licence issued by the Bank of Russia; • an information exchange participant operating as a payment infrastructure service provider – the payment infrastructure service operator's registration number | <pre>'participant': {</pre> | [0] | [1], [2] |

| of payment | 'orgOgrn': '1234567890000', |
|-------------------------|---|
| infrastructure; | 'isp': [{ |
| an information | 'name': 'telecom operator name, |
| exchange participant | 'ipAddress': ['192.168.1.0', |
| operating as a payme | nt '192.168.2.0'] |
| system operator – the | |
| payment system | 'software': [{ |
| operator's registration | n 'sourceld': 'f34030ef-358a-445c- |
| number; | 8567- |
| an information | 25985ce6d91c', |
| exchange participant | 'type': 'type of software/hardware of an |
| operating as a | information exchange participant', |
| professional securities | 'name': 'name of software/hardware', |
| market participant – t | he 'version': 'software/hardware version used', |
| number of the licence | |
| issued by the Bank of | software/hardware' |
| Russia; | }], |
| an information | 'persons': [{ |
| exchange participant | 'memberld': '9527dd0c-0765-4f1c- |
| operating as the | 8f5f- |
| management compan | y of 70a02cf4046c', |
| an investment fund, a | ' 'sourceld': 'f34030ef-358a-445c- |
| unit investment fund | and 8567- |
| a non-governmental | 25985ce6d91c', |
| pension fund – the | 'ílastName': 'surname', |
| number of the licence | |
| issued by the Bank of | 'firstName': 'name', |
| Russia; | 'landlineNumber': '1234567890000', |
| an information | 'mobileNumber': |
| exchange participant | '1234567890000', 'email': |
| operating as a | 'qwerty1@example.ru', |
| specialised depository | |
| an investment fund, a | |
| unit investment fund | account of an information exchange participant', |
| and a non-governmer | |
| pension fund – | the responsible person of an information exchange participant' |
| the number of the | <pre>incresponsible person of an information exchange participant }],</pre> |
| licence issued by the | 'id_cii': 'CII object identifier', |
| Bank of Russia; | 'orgType': 'information exchange participant type', |
| an information | (legalAddress': { |
| exchange participant | 'oktmo': '12345678', |
| | 'postalCode': 'postal code', 'country': |
| operating as a | 'three-letter country code', |
| | 'federalDistrict': 'federal district code', |
| | |

| an insurance entity number of the licen issued by the Bank of Russia; an information exchange participan operating as a non- governmental pensi fund - the number of licence issued by the Bank of Russia (a directory of financia market participants) an information exchange participan operating as a microfinance organisation - the registration number the record in the stat register of microfina organisations; an information exchange participar operating as a consu credit cooperative, - OGRN; an information exchange participar operating as a housi savings cooperative - OGRN; an information exchange participar operating as a credi history bureau - the number in the state register of credit history bureaus; an information | see 'cityDistrict': 'inner city district', 'locality': f 'residential area', 'street': 'street', 'house': 'house number', t 'building': 'block/building', 'room' 'room/office', on 'additionalInformation': 'additional information' } ; } information' } ; } information' } ; } information' } ; } information' * ; } information' * ; } ; } information' * ;; ` information' * ;; ` information ` ;; ` ;; ` |
|--|--|
|--|--|

| exchange participant | | 'district': 'district', | |
|---|--------------|--|--|
| operating as an insurance | | 'city': 'city', | |
| entity - the number of the | | 'cityDistrict': 'inner city district', 'locality': | |
| licence issued by the Bank | | 'residential area', | |
| of Russia; | | 'street': 'street', 'house': | |
| an information | | 'house number', | |
| exchange participant | | 'building': 'block/building', 'room' | |
| operating as a non- | | 'room/office', | |
| governmental pension | | 'additionalInformation': 'additional | |
| fund - the number of the | information' | | |
| licence issued by the | } |] | |
| Bank of Russia (a | } | | |
| directory of financial | } | | |
| market participants); | | | |
| an information | | | |
| exchange participant | | | |
| operating as a | | | |
| microfinance | | | |
| organisation - the | | | |
| registration number of | | | |
| the record in the state | | | |
| register of microfinance | | | |
| organisations; | | | |
| an information | | | |
| exchange participant | | | |
| operating as a consumer | | | |
| credit cooperative, | | | |
| – OGRN; | | | |
| an information | | | |
| exchange participant | | | |
| operating as a housing | | | |
| savings cooperative | | | |
| – OGRN; | | | |
| OGRN; an information | | | |
| an information exchange participant | | | |
| | | | |
| operating as a credit history bureau – the | | | |
| number in the state | | | |
| number in the state | | | |
| | | | |
| | | | |
| | | | |

| register of credit history | | |
|---|--|--|
| bureaus; | | |
| an information | | |
| exchange participant | | |
| operating as an actuary – | | |
| the registration number | | |
| of the record on entering | | |
| information in the | | |
| unified register of | | |
| responsible actuaries; | | |
| an information | | |
| exchange participant | | |
| operating as a credit | | |
| rating agency - number | | |
| of the issued form of the | | |
| certificate of entry of | | |
| information about the | | |
| legal entity in the | | |
| register of credit rating | | |
| agencies; | | |
| an information | | |
| exchange participant | | |
| operating as an | | |
| agricultural consumer | | |
| credit cooperative – | | |
| number in the state | | |
| register of agricultural consumer credit | | |
| cooperatives; | | |
| an information | | |
| exchange participant | | |
| operating as a | | |
| pawnshop – number in | | |
| the state register of | | |
| pawnshops; | | |
| information | | |
| exchange participant | | |
| (state authorities, | | |
| foreign organisations, | | |
| | | |
| | | |

| | | | providers, software |
|----------------|---------------------------------|-------------------------|--------------------------------|
| | | | developers, centres of |
| | | | competence for |
| | | | countering cyber threats) |
| | | | – full name of the |
| | | | organisation |
| | | | |
| | 'orgBrand' | name of the | textarea (text field) |
| | (data field) | information | |
| 2.2 | | exchange | |
| | | participant's | |
| | | brand | |
| | () | - | |
| | 'orgShortName' | | textarea (text field) |
| 2.2 | (data field) | the | |
| 2.3 | | information | |
| | | exchange participant | |
| 2.4 | (| | ++ |
| 2.4 | ʻorgFullName' (data field) | | textarea (text field) |
| | (uata neiu) | an information | |
| | | | |
| | | exchange participant | |
| 2.5 | 'orgEmails' | | Addresses of electronic |
| 2.5 | (data field) | group | mailboxes of an |
| | (uata nelu) | | information exchange |
| | | an | participant shall be |
| | | information | submitted in the format in |
| | | | accordance with |
| | | exchange | |
| | | participant | Specification RFC 5322 |
| 2.6 | 'orgIncomingEmail | the | [18] The e-mail address for |
| 2.0 | (data field) | information | receiving messages from |
| | (uata nelu) | exchange | the Bank of Russia shall be |
| | | | submitted in the format in |
| | | mailbox | accordance with |
| | | | Specification RFC 5322 |
| | | address for | [18] |
| | | receiving | [10] |
| | | messages | |
| | | from the Bank of | |
| | | Russia | |
| 2.7 | 'orgBik' | BIC of the | in the AAAAAAAA |
| | (data field) | information | format |
| | | exchange | lonnat |
| | | participant | |
| Mandatory noti | fication is established only fo | | |

1 Mandatory notification is established only for credit institutions.

| 2.8 | ʻorgLegalEntityF or m' (data field) | OKOPF code of the information exchange participant | in the five-digit format – XXXXX |
|--------|---|---|---|
| 2.9 | ʻorgBin' (data field) | BIN of the information exchange participant | in the six-digit format – XXXXXX |
| 2.10 | ʻorgInn' (data field) | TIN of the information exchange participant | in the XXXXXXXXXX format |
| 2.11 | ʻorgKpp' (data field) | KPP (tax registration reason code) of the exchange participant | in the nine-digit code format – NNNNPPXXX |
| 2.12 | ʻorgOgrn' (data field) | OGRN of the information exchange | in the 13-digit format CFFKKHHXXXXXY |
| 2.13 | ʻlsp'(data block) | telecom operator's identifier | If it is necessary to specify several values of data fields (name, ipAddress), specify one or several objects in the data block 'isp' |
| 2.13.1 | 'name' (data field) | telecom operator name | textarea (text field) |
| 2.13.2 | ʻipAddress' (data field) | external IP addresses of the information exchange participant | Logical addresses of type IPv4 shall comply with Specification RFC 791 [12] |
| 2.14 | ʻsoftware' (data block) | composition of software/har dware used | If it is necessary to specify several data field values (sourceld, type, name, version, description), specify one or several objects in the 'software" data block |

| 2.14.1 | 'sourceld' identifier (data field) assigned b the informatic exchange participar | y generated in accordance with Specification RFC 14122 [16] assigned by the information exchange participant |
|--------|---|---|
| 2.14.2 | | 1) System levels. |

| 2.14.3 | 'name' | name of | conducted by using payment cards, [web] – information resources of the Internet, [abs] – automated banking system, [back-office] – system for post- transaction servicing of payment card transactions, [int-services] – internal information infrastructure for supporting business processes of an information exchange participant (mail servers, file servers); [participant_w] – terminal equipment (AWS) used by employees of an information exchange participant. | | |
|--------|---------------------------|---------------------------------------|---|-----|----------|
| 2.14.3 | name (data field) | name of software/ hardware used | | [N] | [1], [2] |
| 2.14.4 | ʻversion' (data field) | software/har dware version used | textarea (text field) | [N] | [1], [2 |

| 2.14.5 | ʻdescription' (data field) | additional description of software/har dware used | textarea (text field) |
|--------|-------------------------------|---|--|
| 2.15 | ʻpersons' (data block) | responsible person identifiers | If it is required to indicate several values of data fields (memberld, sourceld, lastName, middleName, firstName, landlineNumber, mobileNumber, email, position, active) one or several objects shall be specified in the 'persons" data block |
| 2.15.1 | ʻmemberld' (data field) | identifier of the responsible person of an information exchange participant assigned by the Bank of Russia | 128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by the Bank of Russia |
| 2.15.2 | ʻsourceld' (data field) | identifier of the responsible person in the information exchange participant system | 128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by the information exchange participant |
| 2.15.3 | 'lastName' | surname | textarea (text field) |
| 2.15.4 | (data field) 'middleName' | middle namo | textarea (text field) |
| 2.15.4 | muuleivaine | muule name | lexialed (lext field) |

| | (data field) | | |
|---------|----------------------------------|--|---|
| 2.15.5 | ʻfirstName' (data field) | name | textarea (text field) |
| 2.15.6 | ʻlandlineNumber' (data field) | stationary telephone | textarea (text field) |
| 2.15.7 | 'mobileNumber' (data field) | mobile telephone | textarea (text field) |
| 2.15.8 | ʻemail' (data field) | e-mail address | textarea (text field) |
| 2.15.9 | 'position' (data field) | position | textarea (text field) |
| 2.15.10 | ʻactive' (data field) | access to the personal account of an information exchange participant | One code shall be selected from the limited set of possible values: • [ACT] – access to the personal account of an information exchange participant is activated; • [DIS] – access to the personal account of an information exchange participant is not activated |
| 2.15.11 | ʻcategory' (data field) | | One code shall be selected from the limited set of possible values: • [MANAGEMENT] – top management; • [SECURITY] – information security units; • [IT] – IT units; • [RISKS] – risk management units; • [PAYMENT] - operational units; • [OTHER] - other structural units |

| 'ID_CII'identifier of atextarea (text field)(data field)CII object | [N] |
|---|-----|
| 'orgType' (data field)type of an information exchange participantOne code shall be selected from the limited set of possible values: • [PSP] is an information exchange participant engaged in the money transfer operator's activity; • [SOPI] is an information exchange participant engaged in the payment infrastructure service provider's activity; • [PS] is an information exchange participant engaged in the payment infrastructure service provider's activity; • [PS] is an information exchange participant engaged in the payment system operator's activity. Non-bank financial institutions: • [PSB] is an information exchange participant engaged in the payment system operator's activity. Non-bank financial institutions: • [PSB] is an information exchange participant engaged in the activity of a professional securities market participant; • [MOF] is an information exchange participant operating as the management company of an investment fund, a unit investment fund, a unit investment fund, a unit investment fund and a non-governmental pension fund; | |



| | operating as an insurance | | |
|--|----------------------------|--|--|
| | operating as an insurance | | |
| | entity; | | |
| | • [NGPF] is an | | |
| | information exchange | | |
| | participant operating as a | | |
| | non-governmental | | |
| | pension fund; | | |
| | • [MFO] is an | | |
| | information exchange | | |
| | participant operating as | | |
| | a microfinance | | |
| | organisation; | | |
| | • [CCC] is an | | |
| | information exchange | | |
| | participant operating as | | |
| | a consumer credit | | |
| | cooperative; | | |
| | • [HCCC] is an | | |
| | information exchange | | |
| | participant operating as a | | |
| | housing savings | | |
| | cooperative; | | |
| | • [CHB] is an | | |
| | information exchange | | |
| | participant operating as | | |
| | a credit history bureau; | | |
| | • [AA] is an | | |
| | information exchange | | |
| | participant engaged in | | |
| | actuarial activities; | | |
| | • [CRA] is an | | |
| | information exchange | | |
| | participant operating as | | |
| | a credit rating agency; | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

| [ACCC] is an | | |
|---------------------------|--|--|
| information exchange | | |
| participant operating as | | |
| an agricultural consume | | |
| credit cooperative; | | |
| • [PWS] is an | | |
| information exchange | | |
| participant operating as | | |
| pawnshop. | | |
| Public authorities: | | |
| • [FED] is an | | |
| information exchange | | |
| participant who is a | | |
| federal executive | | |
| authority; | | |
| • [REG] is an | | |
| information exchange | | |
| participant who is an | | |
| executive authority of a | | |
| constituent entity of the | | |
| Russian Federation; | | |
| • [localGov] is an | | |
| information exchange | | |
| participant who is a | | |
| local government; | | |
| • [LEA] is a law | | |
| enforcement agency. | | |
| Telecom operators: | | |
| • [MO] is an | | |
| information exchange | | |
| participant who is a | | |
| cellular mobile operator | | |
| • [ISP] is an | | |
| information exchange | | |
| participant who is an | | |
| Internet provider; | | |
| | | |
| Software developers: | | |
| • [devBANK] is an | | |
| information exchange | | |
| participant – a eveloper | | |
| of application software | | |

| for financial (banking) | | |
|--------------------------------------|--|--|
| activities; | | |
| [devVIRUS] is an | | |
| information exchange | | |
| participant – a developer | | |
| of anti-malware tools | | |
| (hereinafter, AMW tools); | | |
| • [devOTHER] is an | | |
| information exchange | | |
| participant an other | | |
| software developer. | | |
| Foreign organisations: | | |
| • [FNB] is an | | |
| information exchange | | |
| participant who is a | | |
| foreign central (national) | | |
| bank; | | |
| • [FB] is an information | | |
| exchange participant a | | |
| foreign bank; | | |
| • [FOTHER] is an | | |
| information exchange | | |
| participant other | | |
| foreign organisation. | | |
| Centres of competence | | |
| for countering cyber | | |
| threats: | | |
| • [CERTRUS] is an | | |
| information exchange | | |
| participant – a Russian | | |
| cyber threat prevention | | |
| centre; | | |
| • [CERTINT] is an | | |
| information exchange | | |
| participant – a foreign | | |
| centre for countering | | |
| 5 | | |
| | | |
| | | |
| | | |

| | | | cyber threats; [OTHER] is an information exchange participant – other organisation | |
|------|-----------------------------------|---|---|-----|
| 2.18 | ʻlegalAddress' (block) | legal address of the Information exchange participant | text fields (textarea) | [0] |
| 2.19 | ʻpostAddress' (data block) | postal address of the information exchange participant | text fields (textarea) | [0] |
| 2.20 | ʻphysicalAddress' (data block) | | text fields (textarea) | [0] |

6. The data submission form used by information exchange participants to inform the Bank of Russia about incidents related to violation of data protection requirements and deadlines for data submission to the Bank of Russia

6.1. Mandatory conditions and time characteristics of information

Mandatory information conditions:

[O] – data block (field) information shall be provided as required;

[N] – data block (field) information shall be provided if it is technically feasible.

Time characteristics of information provision (stages of information provision):

[1] – data block (field) information shall be provided as part of the initial notification (for important entities of the critical information infrastructure, the information shall be sent to the Bank of Russia within three hours from the moment of incident detection, for other information exchange participants within 24 hours from the moment of incident detection);

[2] – data block (field) information shall be provided as part of an interim notification (for important entities of the critical information infrastructure, the information shall be sent to the Bank of Russia within three hours after the incident is detected, for other information exchange participants within two business days after the initial notification or the previous interim notification);

[3] – data block (field) information shall be provided as part of the final notification of the results of the incident closure (within three business days from the moment of the incident closure by an information exchange participant).

[*] – data block (field) information shall be provided promptly upon receiving from an information exchange participant's client who is a legal entity the notification specified in Part 11 of Article 9 of Federal Law No. 161-FZ, dated 27 June 2011, 'On the National Payment System'.

6.2. Incident identification data. Data block [HEADER]

| Data block (field) No. | ldentifier of data block (field) | Content of data block (field) | Data field format | E-mail format | Obligation of informing | Stages of information provision |
|---------------------------------|-------------------------------------|--|-----------------------|--|----------------------------|---------------------------------------|
| 1 | 'schemaType' | type of | Specify the value of | { | (0) | |
| .1 | (data field) | electronic message | [INCIDENT] - incident | 'header': { 'schemaType': 'incident', | [0] | [1], [2], [3], [*] |
| 1.2 | 'schemaVersion' (data field) | version of electronic message version | textarea (text field) | 'schemaVersion': '1', 'version': '1', 'memberid': '9527dd0c-0765-4f1c-8f5f- 70a02cf4046c', 'sourceld': 'f34030ef-358a-445c- | [0] | [1], [2], [3], [*] |
| 1.3 | 'version' (data field) | version number of electronic | numeric value (int) | 8567-25985ce6d91c', 'publishedAt': '2002-10- 02T15:00:00.05Z', 'modifiedAt': '2002-10-02T15:00:00.05Z' | [0] | [1], [2], [3], [*] |

| | | message during information exchange | | }, | | |
|----|-------------------------------|---|---|----|-----|---|
| 4 | 'memberld' (data field) | information exchange participant identifier | 128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by the Bank of Russia | | [0] | |
| .5 | 'sourceld' (data field) | identifier assigned by an information exchange | 128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by an information exchange participant | | [0] | |
| .6 | ʻpublishedAt' (data field) | time of | data provision format in accordance with Specification RFC 3339 [11] | | [0] | 1 |
| 7 | ʻmodifiedAt' (data field) | of interim or | data provision format in accordance with Specification RFC 3339 [11] | | [0] | |

6.3. Incident description Data Block [INCIDENT]

| Data block (field) No. | ldentifier of data block (field) | Content of data block (field) | Data field format | E-mail format | Obligation of informing | Stages of information provision |
|---------------------------------|-------------------------------------|--|-----------------------|--|----------------------------|---------------------------------------|
| 2.1 | ʻfincertId' (data field) | Incident identifier assigned by the Bank of Russia | textarea (text field) | 'incident': { | [0] | [2], [3] |
| 2.2 | 'fixationAt' | date and time of | data provision format | 'addressed': information exchange participant's appeal to | [0] | [1], [2], [3], [*] |

| | (data field) | incident | in accordance with | law enforcement agencies', | | |
|-------|-----------------|----------------|---------------------------|--|-----|--------------------|
| | . , | registration | Specification RFC 3339 | 'request': 'information on the fact of an | | |
| | | by an | [11] | information exchange participant's appeal to the police', | | |
| | | information | | 'number': '123123', | | |
| | | exchange | | 'numberTicket': '1234567890', 'dateTimeAt': | | |
| | | participant | | '2002-10-02T15:00:00.05Z' | | |
| 2.3 | 'description' | incident | textarea (text field) | }, | [0] | [1], [2], [3], [*] |
| | (data field) | description | | 'assistance': 'identifier of the need to support an | [0] | [1], [2], [3], [] |
| 2.4 | 'lawEnforcement | | | information exchange participant by the Bank of Russia', | | |
| | Request' | information | | 'vectorCode': 'computer attack vector | | |
| | (data block) | exchange | | identifier', | | |
| | | participant's | | 'serviceType': [{ | [0] | [2], [3] |
| | | appeal to law | | 'sourceId': 'f34030ef-358a-445c-8567- | | |
| | | enforcement | | 25985av6d91c', | | |
| | | agencies | | 'type': 'type of attacked object', | | |
| 2.4.1 | 'addressed' | | One code shall be | 'name': 'name of software | | |
| | (data field) | applied to law | selected from the limited | /hardware', | | |
| | | enforcement | set of possible values: | 'version': 'software/hardware | | |
| | | agencies | • [PIE] - information | version', | [0] | [0] [0] |
| | | | exchange participant; | 'description': 'additional description of the | [O] | [2], [3] |
| | | | • [CIE] - client of an | type of | | |
| | | | information exchange | the object under attack' | | |
| | | | participant | }], | | |
| 2.4.2 | 'request' | information | One code shall be | 'registration': { | | |
| 2.7.2 | (data field) | on the fact of | selected from the limited | 'department': 'the structural (organisational) | | |
| | (uata neid) | an | set of possible values: | unit of an information exchange participant where the incident was | | |
| | | information | | registered (detected)', | | |
| | | exchange | [POL] - an appeal to | 'technicalDevice': 'technical tools of | | |
| | | participant's | law enforcement | incident registration' | [0] | [2], [3] |
| | | appeal to law | agencies; | }, | | |
| | | enforcement | • [NPL] - no appeal to | 'typeOfAttack': 'computer attack type code', | | |
| | | agencies | law enforcement | 'measuresAndRecomendations': [{ | | |
| | | ageneies | agencies | 'sourceId': 'f34030ef-358a-445c-8567- | | |
| 2.4.3 | 'number' | application | numeric value (int) | 25985ce6d91c', | | |
| | (data field) | number from | | 'dateTimeAt': '2018-03-22T08:14:38Z', | | |
| | , | the register | | 'action': 'actions taken to eliminate | [0] | [2], [3] |
| | | of crime | | the incident', | | |
| | | reports | | 'text': 'the text of measures taken or | | |
| 2.4.4 | 'numberTicket' | | numeric value (int) | recommendations received', | | |
| | (data field) | ticket for | | - | | (2) (2) |
| | (1.000.000) | accepting and | | 'attachment': { | [0] | [2], [3] |
| | | registering | | 'sourceld': 'f34030ef-358a-445c- | | |
| | | | | 8567- | | |

| | | applications | | 25985ce6d91c', | | |
|-------|-------------------------------|--|---|--|-----|--------------------|
| 2.4.5 | 'dateTimeAt' (data field) | date and time of the application acceptance | data provision format in accordance with Specification RFC 3339 [11] | 'comment': 'description of the attachment', 'dateTimeAt': '2018- 03-22T08:14:38Z', 'file': { | [0] | [2], [3] |
| 2.5 | 'assistance' (data field) | identifier of the need to support an information exchange participant by the Bank of Russia | One code shall be selected from the limited set of possible values: • [HLP] - support from the Bank of Russia is needed; • [NND] - no support required from the Bank of Russia | 'name': 'file name', 'size': 'file size in bytes', 'base64': 'attachment in base64 format' }, 'fileLink': 'http://domain.com/archive.rar' } }}, | [0] | [1], [2], [3], [*] |
| 2.6 | 'vectorCode' (data field) | computer attack vector identifier | One code shall be selected from the limited set of possible values: • [INT] – vector aimed at the information exchange participant infrastructure; • [EXT] – vector aimed at an information exchange participant's client | | [0] | [1], [2], [3], [*] |
| 2.7 | 'serviceType'(data block) | information infrastructur e object identifier | If it is necessary to specify several data field values (sourceld, type, name, version, description), one or several objects in the data block 'serviceType' should be specified | | [0] | [1], [2], [3], [*] |
| 2.7.1 | ʻsourceld' (data field) | identifier assigned by an information exchange participant | 128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by an information exchange | | [0] | [1], [2], [3], [*] |
| | | | narticipant |
|-----|----------------|----|---|
| | | | participant |
| 7.2 | 'type' type of | | One code shall be |
| | | | selected from the limited |
| | attac | :k | set of possible values: |
| | | | 1) system levels: |
| | | | |
| | | | • [hw] - hardware, |
| | | | • [net] - network |
| | | | equipment, |
| | | | • [net_s] – network |
| | | | applications and |
| | | | services, |
| | | | • [hw _ s] – server |
| | | | components of |
| | | | virtualisation, software |
| | | | infrastructure services, |
| | | | • [os] - operating systems, database |
| | | | management systems, |
| | | | application servers; |
| | | | application servers, |
| | | | 2) the level of AS |
| | | | and applications used to |
| | | | provide services within |
| | | | the framework of |
| | | | business or technological |
| | | | processes of an |
| | | | information exchange participant: |
| | | | |
| | | | • [rbs] – remote |
| | | | banking system, |
| | | | • [front-office] - payment card transaction |
| | | | processing system, |
| | | | • [web] - information |
| | | | resources of the |
| | | | resources of the |
| | | | |
| | | | |
| | | | |

| Internet | | | |
|----------------|--------------|--|--|
| Internet, | | | |
| • [abs] - a | | | |
| banking syst | | | |
| • [back-of | | | |
| system of po | | | |
| transaction | | | |
| operations of | | | |
| using payme | | | |
| • [int-serv | ces] – | | |
| internal info | nation | | |
| infrastructu | for | | |
| supporting b | siness | | |
| processes of | in | | |
| information | xchange | | |
| participant (| ail servers, | | |
| file servers); | | | |
| • [particip | nt _ w] - | | |
| terminal equ | | | |
| (AWS) used | | | |
| employees of | | | |
| information | | | |
| participant; | C . | | |
| | | | |
| 3) the le | el of the AS | | |
| and applicat | ons operated | | |
| by an inform | tion | | |
| exchange pa | cicipant's | | |
| client: | | | |
| • [cfs] - fil | server, | | |
| • [crbs] – | | | |
| banking syst | | | |
| • [ecs] - e | | | |
| server; | | | |
| • [client _ | v] - | | |
| automat | | | |
| systems use | | | |
| employees of | | | |
| information | | | |
| Information | | | |
| | | | |
| | | | |

| | | exchange participant's client; 4) other system: |
|-------------------|---|--|
| | | |
| | | 4) other system: |
| | | 4) other system: |
| | | |
| | | • [oth] - other system |
| | | |
| | 'name of | textarea (text field) |
| | software | |
| | hardware | |
| | - | |
| | | textarea (text field) |
| (data field) | | |
| | version | |
| | 1.1 | |
| | | textarea (text field) |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| 'department' | the attacked | textarea (text field) |
| | structural | , , |
| | (organisationa | |
| | | |
| | | |
| | | |
| | | |
| | where an | |
| | incident was | |
| | | |
| | (detected) | |
| | | |
| 'technicalDevice' | technical | textarea (text field) |
| (data field) | tools of | |
| | incident | |
| | registration | |
| 'typeOfAttack' | Computer | One code shall be |
| | | |
| | attack type identifier | selected from the limited set of possible values: |
| | 'department' (data field) 'technicalDevice' (data field) | (data field)hardware version'description' (data field)additional description of the type of an attacked object'registration' (data block)incident localisation identifier'department' (data field)the attacked structural (organisationa l) unit of an information exchange participant where an |

| [trafficHijackAttacks] | | |
|---------------------------|--|--|
| – computer attacks | | |
| related to changes in | | |
| route and address | | |
| information; | | |
| • [malware] – | | |
| computer attacks related | | |
| to the use of malicious | | |
| software in relation to | | |
| information | | |
| infrastructure objects of | | |
| information exchange | | |
| participants and their | | |
| clients; | | |
| [socialEngineering] | | |
| computer attacks | | |
| launched after inducing | | |
| customers to make | | |
| money transfers by | | |
| deceit or breach of trust | | |
| • [ddosAttacks] – | | |
| denial-of-service | | |
| computer attacks (DDoS | | |
| attacks) in relation to | | |
| the information | | |
| infrastructure of | | |
| information exchange | | |
| participants; | | |
| • [atmAttacks] – | | |
| computer attacks related | | |
| to unauthorised access | | |
| to ATMs and payment | | |
| terminals of information | | |
| exchange participants; | | |
| | | |
| | | |
| | | |
| | | |
| | | |

| • [vulnerabilities] – | |
|---|--|
| computer attacks related | |
| to the full use of | |
| vulnerabilities (exploiting | |
| vulnerabilities) of the | |
| information | |
| infrastructure of | |
| information exchange | |
| participants and their | |
| clients for the benefit of | |
| an attacker; | |
| • [bruteForces] – | |
| computer attacks related | |
| to searching (hacking) | |
| and compromising | |
| authentication data | |
| (login details); | |
| • [spams] – computer | |
| attacks related to | |
| spamming information | |
| exchange participants | |
| and their customers; | |
| • [controlCenters] – | |
| computer attacks related | |
| to the detection of | |
| interaction of | |
| information | |
| infrastructure objects of | |
| information exchange | |
| participants with Botnet | |
| command centres; | |
| • [sim] – computer | |
| attacks associated with | |
| the change (substitution) | |
| of the mobile subscriber | |
| identifier (IMSI) of the | |
| SIM card number, as well | |
| as with the replacement | |
| of the mobile equipment | |
| identifier (IMEI); | |
| [phishingAttacks] – | |

| computer attacks | |
|----------------------------|---|
| associated with data that | |
| are deceptive for | |
| information exchange | |
| participants and their | |
| clients, as well as other | |
| persons interacting with | |
| them, regarding the | |
| ownership of information | |
| distributed via the | |
| Internet due to the | |
| similarity of domain | |
| names, design or | |
| content; | |
| • [prohibitedContents] – | |
| computer attacks | |
| associated with the | |
| distribution of | |
| information regarding | |
| the offer and/or | |
| provision of financial | |
| services in the Russian | |
| Federation by persons | |
| not entitled to provide | |
| them in accordance with | |
| the legislation of the | |
| Russian Federation. | |
| Posting of prohibited | |
| content on the Internet; | |
| • [maliciousResources] | |
| – computer attacks | |
| associated with the | |
| placement on the | |
| Internet of information | |
| enabling illegal access to | |
| information systems of | |
| information exchange | |
| participants and their | |
| customers used in the | |
| provision (receipt) of | |
| | |
| | _ |

| | | | financial services, including through illegal access to confidential customer information. Placement of a malicious resource on the Internet; • [changeContent] – computer attacks related to a change in content; • [scanPorts] – computer attacks related to scanning software ports of information infrastructure objects of information exchange participants by persons who do not have the relevant authority; • [other] – other computer attacks directed to information infrastructure objects of information exchange participants and their clients | | |
|--------|----------------------------------|-------------------------------|--|-----|---------------|
| 2.10 | 'measuresAndRe- comendations' | actions taken to eliminate | If it is necessary to specify several data field values | | |
| | (data block) | an incident | (sourceld, data field values (sourceld, dateTimeAt, action, text), one or several objects in the data block 'measuresAndRecomend ations' are to be specified | [N] | [1], [2], [3] |
| 2.10.1 | 'sourceld' | Identifier | 128-bit identifier | [N] | [1], [2], [3] |

| | (data field) | assigned by | (GUID) generated in |
|----------|------------------------|-----------------------------|---|
| | | an | accordance with |
| | | information | Specification RFC 4122 |
| | | exchange | [16] assigned by the |
| | | participant | information exchange |
| | | | participant |
| 2.10.2 | 'dateTimeAt' | date and | data provision format in |
| | (data field) | time of actions | accordance with Specification RFC 3339 |
| | | taken to | [11] |
| | | eliminate an | [++] |
| | | incident | |
| 2.10.3 | 'action' | actions taken | One code shall be |
| | (data field) | to eliminate | selected from the limited |
| | | an incident | set of possible values: |
| | | | • [measures] – the |
| | | | measures taken; |
| | | | [recommendations] - |
| 2.40.4 | | | recommendations |
| 2.10.4 | 'text' (data field) | measures taken or | textarea (text field) |
| | (uata neiu) | recommendati | |
| | | ons followed | |
| 2.10.5 | 'attachment' | additional | |
| | (data block) | data on the | |
| | | measures | |
| | | taken to | |
| | | eliminate an incident | |
| 2.10.5.1 | | identifier | 128-bit identifier (GUID) |
| 2.10.5.1 | | assigned by | generated in accordance |
| | | an | with Specification RFC |
| | 'sourceld' | information | 4122 [16] assigned by the |
| | (data field) | exchange | information exchange |
| | | participant | participant |
| | | | |
| 2.10.5.2 | 'comment' | description of | textarea (text field) |
| | (data field) | the | |
| 2.10.5.3 | | attachment date and time | data provision format in |
| 2.10.3.3 | 'dateTimeAt' | when the file | accordance with |
| | (data field) | was added | Specification RFC 3339 |
| | | | [11] |
| | | | |

6.4. Incident classification. Data Block [INCIDENT]

| Data block (field) No. | ldentifier of data block (field) | Content of data block (field) | Data field format | E-mail format | Obligation of informing | Stages of information provision |
|---------------------------------|---|--|--|---|----------------------------|---------------------------------------|
| 3.1 | 'location' (data block) | identifier of the geographical location of the incident | | 'location': { | [0] | [1], [2], [3], [*] |
| 3.1.1 | ʻsubjectOf Federatio n' (data field) | upper-level OKTMO code | textarea (text field) | 'ext': [{ | [0] | [1], [2], [3], [*] |
| 3.1.2 | 'locality' (data field) | name of a residential area | textarea (text field) | and transferring operational instructions enabling financial transactions' }], | [0] | [1], [2], [3], [*] |
| 3.2 | 'classification' (data block) | incident classification | | 'int': [{ 'events': 'data protection | [0] | [1], [2], [3], [*] |
| 3.2.1 | 'typeOfIncident' (data field) | incident type | One code shall be selected from the limited set of possible values: • [MTR] – an incident involving a violation of the information protection requirements when making money transfers; when making | events', 'typeOfIntruder': 'intruder type' }], 'damage': { 'operating': 'assessment of operational expenses of an information exchange participant at the moment of providing data on the occurrence of an incident (INT vector)', | [0] | [1], [2], [3], [*] |

| | | | money transfers: | (relative): (relative (qualitative) | | |
|---------|--------------------------|------------------------------|---|--|-----|--------------------|
| | | | money transfers; [BAC] – an incident involving a violation of the information protection requirements in the course of banking activities; [FMA] – an incident involving a violation of the information protection requirements in financial markets; [DT_MTR] – an incident involving the non-provision or untimely provision of money transfer services; [DT_FS] – an incident related to a failure to provide financial services or their untimely provision | <pre>'relative': 'relative (qualitative) assessment of the scale (severity of consequences) of an incident (INT vector)', 'schemaConclusion': 'description of a money withdrawal scheme', 'attachments': [{ 'sourceld': 'f34030ef-358a-445c- 8567- 25985ce6d91c', 'comment': 'description of the attachment', 'dateTimeAt': '2018- 03-22T08:14:38Z', 'file': { 'name': 'file name', 'size': 'file size in bytes', 'base64': 'attachment in base64 format' }, 'fileLink': 'http://domain.com/archive.rar' }]</pre> | | |
| 3.2.2. | 'ext' (data subblock) | an incident involving an | If it is necessary to specify several data field values (events, method), specify one or several objects in the 'ext' data sub-block | }, | [0] | [1], [2], [3], [*] |
| 3.2.2.1 | 'events' (data field) | data protection events | One code shall be selected from the limited set of possible values: • [MTR _ WC] – receipt by the money transfer operator servicing the payer, including the electronic money operator, of notifications in the form stipulated by the agreement from | | [0] | [1], [2], [3], [*] |



| | | | the Bank of Russia | |
|-------|--------------|--------------|----------------------------|-----|
| | | | website; | |
| | | | • [FMA _ WC] – receipt | |
| | | | of notifications from | |
| | | | customers: individuals, | |
| | | | and (or) individual | |
| | | | entrepreneurs, and (or) | |
| | | | individuals engaged in | |
| | | | private business in | |
| | | | accordance with the | |
| | | | procedure established by | |
| | | | the legislation of the | |
| | | | Russian Federation, and | |
| | | | (or) legal entities about | |
| | | | conducting a financial | |
| | | | (banking) transaction | |
| | | | without their consent; | |
| | | | • [OTH] – other events | |
| | | | the consequences or | |
| | | | identification of which | |
| | | | may lead to incidents | |
| | | | specified in codes [MTR], | |
| | | | [BAC], [FMA], [DT_ | |
| | | | MTR], [DT_FS] | |
| | | | wing, [01_13] | |
| 2.2.2 | 'method' | a method of | One code shall be | |
| | (data field) | creating and | selected from the limited | |
| | | transferring | set of possible values: | |
| | | operational | • [SMS] is a remote | |
| | | instructions | service technology | |
| | | enabling a | where information is | |
| | | financial | exchanged between an | |
| | | transaction | information exchange | [0] |
| | | | participant and its client | |
| | | | using short text | |
| | | | messages from the | |
| | | | telephone number | |
| | | | specified in the bank | |
| | | | specified in the ballk | |
| | | | account agreement; | |



| | | | [CIN] is an ATM capable to accept cash; [REC] is an ATM with a recycling function; [POS] is a POS terminal; [SST] is a payment terminal; [CNP] is making transfers using payment cards without their direct use (CNP transactions); [OTH] is another method of creating and transferring transaction instructions enabling a financial transaction |
|---------|--------------------------|---|---|
| | 'int' (data subblock) | an incident in the information infrastructure of an information exchange participant | |
| 3.2.3.1 | 'events' (data field) | infrastructure of an information exchange participant data protection | several objects in the 'int' data sub-block shall be specified One code shall be selected from the limited |
| | | events | [MTR_UA] – identification by the money transfer operator servicing the payer, including |

| the electronic money operator, of money transfer operations and cash receipts as a result of unauthorised access to the information infrastructure of the money transfer operator, including when the balance of electronic funds is reduced, except for virtual payment cards; • [FMS_UA] – conducting financial (banking) operations as a result of unauthorised access to information infrastructure facilities of a non-bank financial institution; • [UPT_PSP] – unauthorised withdrawal of funds of the money transfer operator from ATMs; • [UPT_EMP] – unauthorised withdrawal of funds of the electronic money operator from ATMs; | | |
|--|--|--|
| | | |

| • [DT_ALL] - |
|----------------------------|
| failure to provide |
| services of the money |
| transfer operator for a |
| period of more than two |
| hours in general for all |
| constituent territories of |
| the Russian Federation |
| where the money |
| transfer operator |
| transfers funds using |
| payment cards, their |
| details and (or) remote |
| banking systems (funds); |
| • [DT_SELECTED] - |
| failure to provide |
| services of the money |
| transfer operator for a |
| period of more than two |
| hours in general for |
| individual constituent |
| territories of the Russian |
| Federation where the |
| money transfer operator |
| transfers funds using |
| payment cards, their |
| details and (or) a remote |
| |
| banking system (s); |
| • [DT_SC] – failure |
| of the settlement centre |
| to provide settlement |
| services for a period of |
| more than one |
| operational day; |
| • [DTPT_SC] – failure |
| by a settlement centre to |
| make payments during an |
| operational day |
| operational day |
| |
| |

| according to orders of a payment clearing centre or payment system participants accepted for execution; | |
|---|--|
| • [DT_CC] – suspension by a clearing centre of the provision of payment clearing services for the period of more than one operational day; | |
| • [DTPT_CC] – failure of a clearing centre to perform payment clearing subject to the accepted orders of the payment system participants during one operational day; | |
| • [DT_OC] – suspension by an operational centre of the provision of operational services for a period of more than two hours; | |
| • [DT_FS_ALL] – non-provision of services by a non-bank financial institution for a period of more than two hours in total for all constituent territories of the Russian Federation where this non-bank financial | |
| institution provides financial (banking) services; • [DT_FS_SEL] – | |
| non-provision of services by a | |

| non-bank financial institution for a period of more than two hours in total for individual constituent territories of the Russian Federation where this non-bank financial institution provides financial (banking) services; | |
|--|--|
| [PSP_CMTR] – detection by a money transfer operator, including an electronic money operator, and/or a payment infrastructure service provider of attacks the consequences of which may lead to events and attempts of making money transfers without their customer's consent; | |
| • [CO_CFS] – detection by a credit institution of computer attacks, the consequences of which may lead to events and attempts to carry out a financial (banking) transaction without its customer's consent; | |
| • [NCFI_CFS] – detection by a non-bank financial institution of computer attacks, the consequences of which may lead to events and attempts to conduct an operation in the | |

| | | | 1 |
|---------|------------------|-------------------|---------------------------|
| | | | financial market without |
| | | | its customer's consent; |
| | | | |
| | | | |
| | | | • [OTH] – other |
| | | | events the |
| | | | |
| | | | consequences or |
| | | | detection of which may |
| | | | lead to incidents |
| | | | specified in codes |
| | | | [MTR], [BAC], [FMA], |
| | | | [DT _ MTR], [DT_FS] |
| 3.2.3.2 | 'typeOfIntruder' | intruder/violato | One code shall be |
| | (data field) | type | selected from the |
| | (| -71 | limited set of possible |
| | | | values: |
| | | | • [INT_ORG] - |
| | | | unauthorised access of |
| | | | employees of an |
| | | | |
| | | | information exchange |
| | | | participant or other |
| | | | persons with the |
| | | | authority to access |
| | | | information |
| | | | infrastructure facilities |
| | | | of an information |
| | | | exchange participant |
| | | | (actions of an internal |
| | | | violator); |
| | | | • [EXT_ORG]- |
| | | | computer attacks or |
| | | | unauthorised access of |
| | | | persons who do not |
| | | | have the authority to |
| | | | access information |
| | | | infrastructure facilities |
| | | | of an information |
| | | | exchange participant |
| | | | (actions of an external |
| | | | violator) |
| 3.3 | 'damage' | identification of | |
| 5.5 | | damages from | |
| | | uamages nom | |

| | | unauthorised | |
|-------|--|---|---|
| | | operations | |
| 3.3.1 | 'operating' (data field) | operational expenses of an information exchange participant at the moment of reporting the incident occurrence (INT vector) | textarea (text field) |
| 3.3.2 | 'relative' (data field) | relative (qualitative) | One code (pursuant to Section 14 hereof) is to be selected from the limited set of possible values: • [MOD] – moderate influence; • [ESS] – essential impact; • [CRIT] – critical impact |
| 3.4 | 'schema Conclusion' (data field) | description of a money withdrawal scheme | textarea (text field) |
| 3.5 | 'attachments' (data block) | additional data for incident identification | If it is necessary to specify several data field values (sourceld, comment, dateTimeAt, file, fileLink), one or several objects in the 'attachments' data block should be specified |

¹ Reporting is mandatory only for non-bank financial institutions.

| 3.5.1 | ʻsourceld' (data field) | identifier assigned by an information exchange participant | 128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by the information exchange participant |
|-------|------------------------------|---|--|
| 3.5.2 | 'comment' (data field) | attachment description | textarea (text field) |
| 3.5.3 | 'dateTimeAt' (data field) | date and time when the file was added | data provision format in accordance with Specification RFC 3339 [11] |
| 3.5.4 | 'file' (data block) | data file | Specify the name and size of the file (no more than 5 MB) and perform Base64 encoding |
| 3.5.5 | 'fileLink' (data field) | link for obtaining (downloading) the data file | |

6.5. 'Antifraud' Data Block [ANTIFRAUD]

The 'antifraud' data block is used by information exchange participants in the following cases:

when money transfer operators, payment system operators, and payment infrastructure service providers inform the Bank of Russia of all events and attempts to transfer funds without their customer's consent [4];

when money transfer operators inform the Bank of Russia of the suspension of funds crediting to a payee's bank account or of the increase in the balance of a payee's electronic funds [20].

| Data block (field) No. | ldentifier of data block (field) | Content of data block (field) | Data field format | E-mail format | Obligation of informing | Stages of information provision |
|---------------------------------|-------------------------------------|---|---|--|----------------------------|---------------------------------------|
| 4.1 | 'antifraud' (data block) | | If it is necessary to specify several data block values (payerldentifier, payer, payee, additionalStatus), one or more objects in the 'antifraud' data block shall be specified | 'sourceld': 'f34030ef-358a-445c- 8567- 25985ce6d91c', 'victim': 'information on the legal status of the payer' | [0] | [1], [2], [3], [*] |
| 4.1.1 | ʻsourceld' (data field) | identifier assigned by an information exchange participant being the payer | 128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by the information exchange participant | 'hashSnils': 'C49337884A71BAB224C7CB438FD7A0D3C1C78AD40664C48F12A9A 8FA441E44' }, 'payer': { 'bik': '123456789', 'inn': '123456789000', 'payerName': 'name of the organisation that is the payer', | [0] | [1], [2], [3], [*] |
| 4.1.2 | 'victim' (data field) | 'information on the legal status of the payer | One code shall be selected from the limited set of possible values: • [person] – an individual; • [entity] – a legal entity | 'payerTransferId': { 'transferType': 'money transfer method type', 'paymentCard': { 'number': '123412341234123412', 'sum': 'amount of a money transfer transaction using | [0] | [1], [2], [3], [*] |

| 4.2 | 'payerIdentifier' | identification | | payment cards', | | | |
|------|-------------------|-----------------|---|--|---------------------------|-----|--------------------|
| | (data block) | data defining | | | 'currency':'currency of | | |
| | | a particular | | money transfers', | | 163 | |
| | | payer | | | 'dateTimeAt': '2018- | [0] | [1], [2], [3], [*] |
| | | paye. | | | 01- | | |
| | | | | 13T09:14:38Z', | | | |
| | | | | | 'rrn': 'the number | | |
| .2.1 | 'hash' | the result of | The sequence of symbols | generated for a money transfer transaction o | luring its authorisation' | | |
| | (data field) | calculating the | obtained as a result of the calculation of the SHA- | | | | |
| | | hashing | 256 hash function from | settle | ement': { | | |
| | | function of | the identification | (12245122451224512245) | 'number': | | |
| | | the number of | document's series and | '12345123451234512345', | 'sum': 'amount of | | |
| | | an | number. | funds to be transforred! | sum : amount of | | |
| | | identification | number. | funds to be transferred', | 'currency':'currency | | |
| | | document in | | of money transfers', | currency currency | | |
| | | order to | The series and number of | or money transfers, | 'dateTimeAt': '2018- | | |
| | | | the identification | | 01-13T09:14:38Z', | | |
| | | identify the | document are to be | }, | 01 10100.14.002 ; | | |
| | | person – the | provided for calculating a | | eNumber': { | | |
| | | payer who | hash function: without | | 'number': | | |
| | | sent the | spaces (_), number sign | '1212312345678', | | | |
| | | notification | (N), letters (if any) in | , , | 'sum': 'transaction | [0] | [1] [2] [2] [*] |
| | | about events | upper case (ABC). | | amount', | [U] | [1], [2], [3], [*] |
| | | and (or) | For a Russian passport, | - | | | |
| | | attempts to | this is XXXXYYYYY , | | 'currency': 'transaction | | |
| | | transfer funds | where: | currency', | | | |
| | | without its | | | 'dateTimeAt': '2018- | | |
| | | | XXXX is the four-digit | | 01-13T09:14:38Z' | | |
| | | client's | passport series number; | }, | | | |
| | | consent, | YYYYYY is the six-digit | ʻidNur | mber': { | | |
| | | including the | passport number. | | 'number': | | |
| | | use of | | '1KoX6AA5VTdbBTkw27YEqKFaTtEQq97AAT' | - | | |
| | | electronic | Source text encoding | | 'sum': 'transaction | | |
| | | means of | (before hash) | | amount', | | |
| | | payment | – Windows-1251; | - | 'currency':'transaction | | |
| | | . , | Hash text encoding - | currency', | currency . transaction | | |
| | | | Windows-1251. | currency, | 'dateTimeAt': '2018- | | |
| .2.2 | 'hash' (data | the result of | The sequence of symbols | | 01- | | |
| .2.2 | | the calculation | | 13T09:14:38Z' | 01 | [0] | [1], [2], [3], [*] |
| | • | of | received as a result of | } | | | |
| | | 01 | | }, | | | |
| | | | | ', 'device': { | | | |



| | | | | Identifier', | | |
|-------|--------------------------------------|---|---|--|-----|--------------------|
| 4.3.1 | 'bik' (data field) | BIC of the money transfer operator, including the e-money operator serving the payer | in the AAAAAAAA format | 'additionalTransactionApprove': ['identifier of additional confirmation of a transaction'] } }], | [0] | [1], [2], [3], [*] |
| 4.3.2 | 'inn' (data field) | TIN of the payer who is a legal entity and/or an individual entrepreneur, and/or a person engaged in private business | for legal entities, in XXXXXXXXXXX or XXXXXXXXXXXXX | | [0] | [1], [2], [3], [*] |
| 4.3.3 | 'payerName' (data field) | organisation name that is the payer | textarea | | [0] | [1], [2], [3], [*] |
| 4.3.4 | 'payerTransferId' (data subblock) | identification data depending on the money | | | [0] | [1], [2], [3], [*] |

| | | transfer method | |
|---------------|----------------------------------|--|--|
| | | method | |
| 4.3.4.1 | 'transferType' (data field) | 'money transfer method type', | One code shall be selected from the limited set of possible values: • [paymentCard] – when making money transfers using payment cards; • [settelment] – when making money transfers to bank accounts; • [phoneNumber] – when making money transfers by telephone number; • [idNumber] – if the balance of electronic funds changes |
| 4.3.4.2 | 'paymentCard' (data subblock) | when making money transfers using payment cards | |
| 4.3.4.2. 1 | 'number' (data field) | the number of the payer's payment card issued to him/her and (or) the person authorised by the payer | in the XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX |

| | | and the money transfer | separation marks (-). |
|---------------|----------------------------|------------------------------|---|
| | | operator by the issuer | |
| 4.3.4.2. | 'sum' | the amount | transaction amount – |
| 2 | (data field) | of a money transfer | field 'F004' of ISO 8583 |
| | | transaction using | Financial Messaging Standard [7], [8], [9] |
| | | payment cards | |
| | | carus | |
| 4.3.4.2. | 'currency' (data field) | currency of a | transaction currency – field 'F049' of ISO 8583 |
| 3 | (data nela) | money transfer | Financial Messaging Standard [7], [8], [9] |
| | | transaction | |
| 4.3.4.2. | 'dateTimeAt' | transaction | data provision format in |
| 4 | (data field) | date and time | accordance with Specification RFC 3339 |
| | | | [11] |
| 4.3.4.2. 5 | 'rrn' (data field) | the number generated for | the number generated for a money transfer |
| | | a money transfer | transaction during its authorisation – field |
| | | transaction during its | 'F037' < * > of ISO 8583 Financial Messaging Standard [7], [8], [9] |
| | | authorisation | Standard [7], [0], [3] |
| | | | * The value of field |
| | | | 'F037' (Retrieval Reference Number) |
| | | | should be generated by |

| | | | the acquiring bank host according to the following rule: YJJJXXNNNNN, where: Y is the last figure of a year; JJJ - a Julian date; XX is the identifier assigned to the acquiring bank's host by the operator; NNNNN - the transaction sequence number during a day | |
|---------------|---------------------------------|--|---|-----|
| 1.3.4.3 | 'settlement' (data subblock) | when making money transfers in bank accounts by debiting funds from payers' bank accounts | | [0] |
| 1.3.4.3. I | 'number' (data field) | the number of the payer's bank account opened with the money transfer operator serving the payer | in the XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX | [0] |

| 4.3.4.3. | 'sum' | | textarea (text field) |
|---------------|----------------------------------|--------------------------|--|
| 2 | (data field) | of a money | |
| | | transfer transaction | |
| 4.3.4.3. | 'currency' | money | textarea (text field) |
| 3 | , (data field) | transfer | |
| | | transaction | |
| | | currency | |
| 4.3.4.3. 4 | 'dateTimeAt' (data field) | transaction | data provision format in accordance with |
| 4 | (uutu nelu) | date and time | Specification RFC 3339 |
| | | time | [11] |
| | | | |
| 4.3.4.4 | 'phoneNumber' (data subblock) | when making | |
| | | money transfers by | |
| | | telephone | |
| | | number | |
| | | | |
| 4.3.4.4. | 'number' | the payer's | in the |
| 4.3.4.4. 1 | (data field) | telephone | KKKXXXNNNNNNN |
| | | number | format, where: |
| | | specified in a | KKK – a country code of |
| | | bank account | one to three characters; |
| | | agreement and/or an | XXX – operator's code; |
| | | agreement on | NNNNNN - seven characters of the |
| | | the use of | number. |
| | | electronic | |
| | | payment | The telephone number is |
| | | instruments concluded | to be provided without a plus sign (+), spaces (_) |
| | | with the payer | |
| | | 1 / - | |

| 4.3.4.4. | 'sum' | transaction | textarea (text field) |
|---------------|-------------------------------|--|---|
| 2 | (data field) | amount | · · · · · · · · · · · · · · · · · · · |
| 4.3.4.4. 3 | (data field) | transaction currency | textarea (text field) |
| 4.3.4.4. 4 | 'dateTimeAt' (data field) | transaction date and time | data provision format in accordance with Specification RFC 3339 [11] |
| 4.3.4.5 | 'idNumber' (data subblock) | if the balance of electronic funds changes | |
| 4.3.4.5. | 'number' (data field) | the payer's identification number, in particular, the number of the payer's electronic wallet used by him/her on the basis of a bank account agreement and (or) an agreement on the use of electronic payment instruments concluded with the money transfer operator | textarea (text field) |

| 4.3.4.5. | 'sum' | 'transaction | textarea (text field) |
|---------------|-------------------|--------------------------|---|
| 4.5.4.5. 2 | (data field) | amount', | |
| 4.3.4.5. | 'currency' | - transaction | textarea (text field) |
| 4.5.4.5. 3 | (data field) | - | lextarea (lext field) |
| 4.3.4.5. | 'dateTimeAt' | transaction | data provision format in |
| 4 | (data field) | date and time | accordance with Specification RFC 3339 |
| | | time | [11] |
| 4.3.5 | 'device' | | |
| | (data subblock) | parameters of the device | |
| | | used to access | |
| | | the | |
| | | automated system and | |
| | | software for | |
| | | the purpose | |
| | | of money transfer | |
| | | without the | |
| | | customer's | |
| | | consent | |
| | | | |
| | | | |
| 4.3.5.1 | 'ip' (data field) | network | The IPv4 network |
| | .p () | address of a | address shall comply |
| | | computer | with Specification RFC |
| | | and/or a communicati | 791 [12] |
| | | on device | |
| | | (router) (IP) | |

| 4.3.5.2 | 'imsi' | International | the number (15-bit |
|---------|--------------|-------------------------|--------------------|
| 4.3.3.2 | (data field) | Mobile | in decimal) |
| | (| Subscriber | AA-BBBBBBB-CCCCCC- |
| | | Identity (IMSI) | |
| | | means the | EE |
| | | international | |
| | | Identifier of | |
| | | a mobile | |
| | | subscriber | |
| | | (individual | |
| | | number of a subscriber | |
| | | (customer – | |
| | | individual) | |
| | | by which | |
| | | the system | |
| | | recognises | |
| | | a mobile | |
| | | communicatio | |
| | | n user using GSM and | |
| | | UMTS | |
| | | standards | |
| | | | |
| 4.3.5.3 | 'imei' | International | the number (15-bit |
| | (data field) | Mobile | in decimal) |
| | , | Equipment | AA-BBBBBBB-CCCCCC- |
| | | Identity (IMEI) | EE |
| | | means the | |
| | | international | |
| | | Identifier of | |
| | | a mobile | |
| | | equipment (a mobile | |
| | | device of an | |
| | | individual | |
| | | customer) | |
| | | | |
| | | | |
| | | | |

| 4.3.5.4 | 'aiic' (data field) | identifier of the participant who is an acquiring bank when transferring funds using payment cards | identifier of the participant who is an acquiring bank in the course of money transfer operations using payment cards (Acquiring institution identification code) - field 'F032' of ISO 8583 [7], [8], [9] | t | [N] | [1], [2 |
|---------|------------------------|---|---|--|-----|----------|
| 4.3.5.5 | 'cati' (data field) | | identifier of the ATM and/or the electronic terminal where the funds are transferred and/or withdrawn (Card acceptor terminal identification) - field 'F041'* of the ISO 8583 Financial Messaging Standard [7], [8], [9] * The value of the terminal identifier shall be aligned to the left and supplemented with spaces on the right with up to 8 characters | c s s r - - D g al d d d s | [N] | [1], [2] |
| 4.3.5.6 | 'caic' (data field) | its | identifier of the ATM and/or electronic terminal where the funds are transferred and/or withdrawn by its geographical location (Card acceptor identification code) - field 'F042'* of ISO 8583 Financial Messaging Standard [7], [8], [9] *The value of the service point identifier shall be aligned to the left and supplemented with spaces on the right with up to 15 characters | e r al d al l, d | [N] | [1], [2] |

| | (| | |
|-------|-------------------------|--|---|
| 4.4 | 'payee' (data block) | information determining the payee | |
| 4.4.1 | 'bik' (data field) | BIC of the money transfer operator serving the payee | in the AAAAAAAA format |
| 4.4.2 | 'inn' (data field) | TIN of the payee - a legal entity, and (or) an individual entrepreneur, and (or) a person engaged in private business | in the XXXXXXXXXX format for legal entities, in XXXXXXXXXXX or XXXXXXXXXXXXXXX formats – for individual entrepreneurs and (or) individuals engaged in private businesses in accordance with the procedure established by the legislation of the Russian Federation |

| 4.4.3 | 'payeeName' (data field) | name of the organisation that is the payee | textarea (text field) |
|---------|--------------------------------------|---|---|
| 4.4.4 | 'payeeTransferld' (data subblock) | identification data depending on the money transfer method | |
| 4.4.4.1 | 'transferType' (data field) | money transfer method type | One code shall be selected from the limited set of possible values: • [paymentCard] – when transferring funds using payment cards; • [settelment] – when transferring funds in bank accounts; • [phoneNumber] – when transferring funds by telephone number; |

| | | | • [idNumber] - if the balance of electronic funds changes |
|---------|---------------------------------|--|---|
| 4.4.4.2 | (data subblock) | when transferring funds using payment cards | |
| 4.4.4.2 | (data field) | the payment card number format of the payee issued to him/her and (or) the person authorised by the payee, the money transfer operator - the issuer | in the format XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX |
| 4.4.4.3 | 'settlement' (data subblock) | when making money transfers in bank accounts by debiting funds from payers 'bank accounts | |
| | · · · · | | |
|---------------|----------------------------------|--|--|
| 4.4.4.3. 1 | 'number' (data field) | the settlement account number of the payee opened with the money transfer operator serving the payee | XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX |
| 4.4.4.4 | 'phoneNumber' (data subblock) | when making money transfers by telephone number | |
| 4.4.4.4. 1 | 'number' (data field) | the payee's phone number | in the KKKXXXNNNNNNN format, where: KKK - a country code of one to three characters; XXX – operator's code; NNNNNNN - seven characters of the number. The telephone number is to be provided without a plus sign (+), spaces (_) and separation signs (-). |
| 4.4.4.5 | 'idNumber' | | and separation signs (-). |
| 4.4.4.5 | lanumber | | |

| | (data subblock) | if the balance of electronic funds changes | |
|----------|------------------------------------|--|--|
| 4.4.4.5. | | number of the payee, in particular, the number of the electronic wallet of the payee used by him/her on the basis of a bank account agreement and (or) an agreement on the use of the electronic means of payment concluded with the money transfer operator | |
| 1.5 | ʻadditionalStatus' (data block) | additional statuses of unauthorised transaction | |
| 4.5.1 | 'crossBorder' | identifier of cross-border banking | |

| | (data field) | | One code is selected from |
|-------|--------------------|--------------|--------------------------------|
| | | | the limited set of possible |
| | | | values: |
| | | | • [CRB] – cross- |
| | | | border transfers; |
| | | | • [DOM] – domestic |
| | | | transfers |
| | | | - |
| 4.5.2 | 'additional Transa | | One or more codes are to |
| | tionApprove' | additional | be selected from the |
| | (data field) | confirmation | limited set of possible |
| | | of a | values: |
| | | transaction | • [3DS] – an operation |
| | | transaction | was confirmed using 3D |
| | | | Secure; |
| | | | • [DCS] - |
| | | | implementation of |
| | | | technological measures |
| | | | to use separate |
| | | | technologies [3]; |
| | | | [NAA] – an |
| | | | operation without |
| | | | confirmation; |
| | | | commation, |
| | | | • [SMS] – an |
| | | | |
| | | | operation was |
| | | | confirmed using short |
| | | | text messages (SMS |
| | | | messages); |
| | | | • [LTR] – an operation |
| | | | was performed in |
| | | | accordance with the list |
| | | | of trusted payees; |
| | | | |
| | | | • [TEL] – an operation |
| | | | was confirmed by |
| | | | telephone; |
| | | | |
| | | | • [OAA] – other |
| | | | method of approval |

6.6. Information on technical data describing computer attacks against information infrastructure facilities of information exchange participants and their customers, as well as relevant forms of electronic messages. Data Block **[IMPACTS]**

6.6.1. Computer attacks related to changes in route and address information [trafficHijackAttacks] (for vector [INT],

[EXT])

| Data block (field) No. | ldentifier of data block (field) | Content of data block (field) | Data field format | E-mail format | Obligation of informing | Stages of information provision |
|---------------------------------|-------------------------------------|---|--|---|----------------------------|---------------------------------------|
| 1.1 | ʻsourceld' (data field) | identifier assigned by an information exchange participant | 128-bit identifier (GUID) generated in accordance with RFC specification 4122 [16] assigned by an information exchange | 'trafficHijackAttacks': [{ 'sourceId': 'f34030ef-358a-445c- | [N] | [2], [3] |
| 1.2 | ʻlegalAsPath' (data field) | legal AS- Path | textarea (text field) | 'lookingGlass': reference link to Looking Glass used to verify AS-Path', | [N] | [2], [3] |
| 1.3 | ʻwrongAsPath' (data field) | wrong AS-Path | textarea (text field) | 'legalPrefix': 'legal prefix', 'wrongPrefix: 'wrong prefix' | [N] | [2], [3] |
| 1.4 | 'lookingGlass' (data field) | reference link to Looking Glass used to verify AS-Path | textarea (text field) | }], | [N] | [2], [3] |
| 1.5 | ʻlegalPrefix' (data field) | legal prefix | textarea (text field) | | [N] | [2], [3] |
| 1.6 | ʻwrongPrefix' (data field) | wrong prefix | textarea (text field) | | [N] | [2], [3] |

6.6.2. Computer attacks related to the use of malicious software for information infrastructure facilities of information exchange participants and their customers **[malware]** (for [INT], [EXT] vector)

| Data block (field) numb | block (field) | Content of data block (field) | Data field format | E-mail format | Obligation of informing | Stages of information provision |
|----------------------------------|---------------|-------------------------------------|--------------------|---------------|----------------------------|---------------------------------------|
| 2 | 'sourceld' | identifier | 128-bit identifier | 'malware': [{ | [N] | [2], [3] |

| | (data field) | assigned by an | GUID) generated in accordance with Specification | 8567-25985ce6d91c', | ef-358a-445c- | | |
|-------|-----------------------------------|---|--|---|-------------------------|-----|----------|
| | | information exchange participant | RFC4122 [16] assigned by an information exchange participant | · 'ip': '127.0 }, | .0.1' | | |
| 2.1 | 'target' (data block) | identifier of the attacked object | | | example.com', | [N] | [2], [3] |
| 2.1.1 | 'ip' (data field) | IP address | The logical IPv4 addressshallcomplyspecification RFC 791 [12] | }], 'classifications': [{ | //example.com' | [N] | [2], [3] |
| 2.2 | ʻsources' (data block) | identifiers of sources of malicious resources on | If it is necessary to specify several data field values (ip, domain, url), one or several objects in the data block | of the AMW tool', 'vendorVei classificatio | | | |
| | | the Internet with which the attacked object interacts | 'sources' should be specified | }], 'malwareSamples' 'hash': { 'mo | : [{ d5': | [N] | [2], [3] |
| 2.2.1 | 'ip' (data field) | IP address | The logical IPv4 address shall comply with Specification RFC 791 [12] | 'D2B063763378A8CB38B192B2F71E78BC13783EF | a1': 'E', a256': | [N] | [2], [3] |
| 2.2.2 | 'domain' (data field) | domain name | Domain name according to Specification RFC 1034 [14] and the international hierarchy of domain zones according to Specification RFC 5890 [13] | 'E25059612A71BAB224C7CB438FD7A0D3C1C78A E48FA441E44' }, 'attachmer 'so 'f34030ef-358a-445c-8567-25985ce6d91c', | | [N] | [2], [3] |
| 2.2.3 | ʻurl' (data field) | URL-address | URL in accordance with Specification RFC 3986 [15] | | mment': scription of | [N] | [2], [3] |
| 2.3 | 'classifications' (data block) | MC classification | If it is necessary to specify several data field values (vendorName, | ʻda 20 03-22T08:14:38Z', | teTimeAt': 18- | | |
| | | | vendorVerdict), one or several objects in the data block 'classifications' should be specified | 'file name', | e': { | [N] | [2], [3] |
| 2.3.1 | 'vendorName' (data field) | name of the MCSE tool used by an information | textarea (text field) | in bytes', 'attachment in base64 format' | size 'base64': | [N] | [2], [3] |
| | | exchange participant | | <pre>attachment in base04 format },</pre> | | | |

| | | | | | 'fileLink': | | |
|---------|---------------------------|----------------------------------|--|--------------------------------|--|------|----------|
| | | | | 'http://domain.com/archive.rar | | | |
| | | | | | } }], 'malwareMessageSenders': [{ | | |
| 2.3.2 | 'vendorVerdict' | MC class in | textarea (text field) | | 'email': 'qwer- | | |
| | (data field) | accordance with the | | ty@example.ru', | 'server': '127.0.0.1' | | |
| | | MCSE tool of | | | }], | [N] | [2], [3] |
| | | an | | | 'malwareMessageAttachment': { | [] | [=]) [0] |
| | | information | | | 'sourceId': 'f34030ef-358a- | | |
| | | exchange | | 445c-8567-25985ce6d91c', | (an an anti-la anna at ta | | |
| 2.4 | 'malwareSamples' | participant it is required to | If it is necessary to specify | the attachment', | 'comment': 'comment to | | |
| | (data block) | | several data field values | | 'dateTimeAt': '2018-03- | | |
| | | | (hash, attachment), one or | 22T08:14:38Z', | | | |
| | | may be | several objects in the data | | 'file': { | [N] | [2], [3] |
| | | | block 'malwareSamples' should be specified | name', | 'name': 'file | נואן | [2], [3] |
| | | function or an | should be speenled | name, | 'size': 'file size | | |
| | | attachment | | in bytes', | | | |
| 2.4.4 | | | | _ | 'base64': | | |
| 2.4.1 | 'hash' (data subblock) | MC sample in the form of | | in base64 format' | 'attachment in | | |
| | Subbiology | hash | | in base04 ionnat | }, | | |
| | | functions | | | 'fileLink': | | |
| | | (MD5, SHA-1, | | 'http://domain.com/archive.ra | r' | [N] | [2], [3] |
| | | SHA-256 function is | | | }, | | |
| | | calculated for | | | 'harmfulResourceAddress': [{ 'ip': '127.0.0.1', | | |
| | | each MC | | | 'domain': 'example.com', | | |
| | | sample) | | | 'url': 'http://example.com' | | |
| 2.4.1.1 | 'md5' | • | sequence of characters | | }], | | |
| | (data field) | the form of MD5 hash | obtained as a result of MD5 hash function calculation | | ʻiocs': [{ | [N] | [2], [3] |
| | | function | | | 'impact': 'type of | | |
| 2.4.1.2 | 'sha1' | | sequence of characters | the detected compromising ide | | | |
| | (data field) | the form of | obtained as a result of the | | 'comment': | [N] | [2], [3] |
| | | | SHA-1 hash function | description' | 'additional | | [2]) [3] |
| 2.4.1.3 | 'sha256' | hash function | calculation sequence of characters | description' | }], | | |
| 2.4.1.3 | (data field) | the form | obtained as a result of | | /1/ 'fil': [{ | [N] | [2], [3] |
| | (| of SHA- 256 | the SHA-256 hash function | | 'impact': 'type of | | [=]/[0] |
| | | | calculation | | the detected | | |

| | | | | Compromising identifier', | | |
|---------------|---|---|--|---|-----|----------|
| 2.4.2 | ʻattachment' (data subblock) | MC sample in the file form of a file | | 'comment': 'additional description' | [N] | [2], [3] |
| 2.4.2.1 | ʻsourceld' (data field) | identifier assigned by an information exchange participant | 128-bit identifier (GUID) generated in accordance with RFC specification 4122 [16] assigned by an information exchange participant | <pre>}],</pre> | [N] | [2], [3] |
| 2.4.2.2 | (data field) | description of the attachment | text field (textarea) | description' }], 'prc': [{ | [N] | [2], [3] |
| 2.4.2.3 | 'dateTimeAt' (data field) | when the file was added | RFC 3339 [11] | 'impact': 'type of the detected compromising identifier', 'comment': | [N] | [2], [3] |
| 2.4.2.4. 1 | 'file' (data subblock) | additional materials containing MC samples | Specify the name and size of the file (no more than 5 MB) and perform Base64 encoding | 'additional description' }], 'oth': [{ 'impact': 'type of | [N] | [2], [3] |
| 2.4.2.5 | 'fileLink' (data field) | additional materials containing MC samples | Specify the URL for downloading the file, if its size exceeds 5 MB, in accordance with Specification RFC 3986 [15] | the detected compromising identifier', 'comment': 'additional description' }] | [N] | [2], [3] |
| 2.5 | 'malwareMessage Senders' (data block) | electronic mailboxes from which | If it is necessary to specify several data field values (email, server), specify one or several objects in the data block 'malwareMessage' | }], 'infectionMethods': [{ | [N] | [2], [3] |
| 2.5.1 | ʻemail' (data field) | sender's e- mail address | The sender's e-mail address shall be submitted in the format in accordance with RFC 5322 specification [18] | }], | [N] | [2], [3] |
| 2.5.2 | 'server' (data field) | IP address of the last mail server | The logical IPv4 address shall comply with Specification RFC 791 [12] | | [N] | [2], [3] |

| 2.6 | "malwareMessage | a file with the | |
|---------|---|---|---|
| 2.0 | Attachment" (data subblock) | initial code of an electronic letter (if MC was sent to the e-mail box) | |
| 2.6.1 | ʻsourceld' (data field) | identifier assigned by an information exchange participant | 128-bit identifier (GUID) generated in accordance with RFC specification 4122 [16] assigned by the information exchange participant |
| 2.6.2 | "comment" (data field) | attachment description | text field (textarea) |
| 2.6.3 | 'dateTimeAt' (data field) | date and time when the file was added | data provision format in accordance with Specification RFC 3339 [11] |
| 2.6.4.1 | "file" (data block) | data file containing a MC sample | Specify the name and size of the file (no more than 5 MB) and perform Base64 encoding |
| 2.6.4 | 'fileLink' (data field) |) a data file containing MC samples | Specify the URL for downloading the file, if its size exceeds 5 MB, in accordance with RFC 3986 specification [15] |
| 2.7 | "harmfulResource- Address" (data block) | identifiers of malicious resources from which a MC was loaded | If it is necessary to specify several data field values (ip, domain, url), specify one or several objects in the data block "harmfulResourceAddress" |
| 2.7.1 | "ip" (data field) | IP address | Logical IPv4 address should comply with Specification RFC 791 [12] |

| | | | 1 |
|---------|--------------------------|--------------------|---|
| 2.7.2 | 'domain' | domain name | Domain name according to |
| | (data field) | | Specification RFC 1034 [14] |
| | | | and the international |
| | | | hierarchy of domain zones |
| | | | according to Specification RFC 5890 [13] |
| 2.7.3 | 'url' | URL-address | |
| 2.7.5 | (data field) | UNL-audress | with RFC 3986 specification |
| | (uutu neiu) | | [15] |
| 2.8 | 'iocs' | identified | If it is necessary to specify |
| | (data block) | compromise | several values of data fields |
| | | indicators | (net, fil, reg, prc, oth), specify |
| | | | one or more objects in the |
| | | | 'iocs' data block |
| 2.8.1 | 'net' | network | If it is necessary to specify |
| 2.0.1 | (data subblock) | | several values of data fields |
| | | maleators | (impact, comment), specify |
| | | | one or several objects in the |
| | | | 'net' data block |
| | | | |
| 2.8.1.1 | 'impact' | type of the | One code shall be |
| | (data field) | compromisin | selected from the limited |
| | | g identifier | set of possible values: |
| | | detected | • [CRT] – creation of |
| | | | technical data; |
| | | | • [UPD] – change in |
| | | | technical data; |
| | | | • [DLT] – technical data |
| | | | deletion |
| 2.8.1.2 | 'comment' | additional | textarea (text field) |
| 202 | (data field) | description | If it is possess to specify |
| 2.8.2 | 'fil' (data subblock) | file indicators | If it is necessary to specify several data field values |
| | SUDDIOCKJ | indicators | (impact, comment), specify |
| | | | one or several objects in |
| | | | the 'fil' data block |
| | | | |
| 2.8.2.1 | 'impact' | type of the | One code shall be |
| | (data field) | compromisin | selected from the limited |
| | | g identifier | set of possible values: |
| | | detected | |

| 2.8.2.2 | 'comment' (data field) | additional description | [CRT] – creation of technical data; [UPD] – change in technical data; [DLT] – technical data deletion textarea (text field) |
|---------|---------------------------|--|---|
| 2.8.3 | 'reg' (data subblock) | OS register indicators | If it is necessary to specify several data field values (impact, comment), specify one or several objects in the 'reg' data block |
| 2.8.3.1 | 'impact' (data field) | type of the compromisin g identifier detected | One code shall be selected from the limited set of possible values: • [CRT] – creation of technical data; • [UPD] – change in technical data; • [DLT] – technical data deletion |
| 2.8.3.2 | 'comment' (data field) | additional description | textarea (text field) |
| 2.8.4 | 'prc' (data subblock) | indicators of OS processes | If it is necessary to specify several data field values (impact, comment), specify one or several objects in the 'prc' data block |
| 2.8.4.1 | 'impact' (data field) | type of the compromisin g identifier detected | One code shall be selected from the limited set of possible values: • [CRT] – creation of technical data; • [UPD] – change in technical data; • [DLT] – technical data deletion |

| 2.8.4.2 | 'comment' | additional | textarea (text field) |
|---------|-------------------|-----------------------------|---|
| | (data field) | description | |
| 2.8.5 | 'oth' | indicators | If it is necessary to specify |
| | (data subblock) | not included in (2.8.1 – | several data field values (impact, comment), specify |
| | | 2.8.4.2) | one or several objects in the |
| | | , | 'oth' data block |
| | | | |
| 2.8.5.1 | 'impact' | type of the | One code shall be |
| | (data field) | compromisin | selected from the limited |
| | | g identifier detected | set of possible values: |
| | | uciccicu | • [CRT] – creation of |
| | | | technical data; |
| | | | [UPD] – change in technical data; |
| | | | [DLT] – technical data |
| | | | deletion |
| 2.8.5.2 | 'comment' | additional | textarea (text field) |
| | (data field) | description | |
| 2.9 | 'infectionMethods | | If it is necessary to specify |
| | (data block) | assumed infection | several data field values |
| | | methods | (impact, comment), specify one or several objects in the |
| | | methous | 'infectionMethods' data |
| | | | block |
| | | | |
| 2.9.1 | 'type' | type of the | One code shall be |
| | (data field) | suspected infection | selected from the limited set of possible values: |
| | | method | |
| | | | [EML] – via e-mails; [DSD] – from a data |
| | | | storage device; |
| | | | • [LCL] – distribution via |
| | | | a local network; |
| | | | • [OTH] – other method |
| | | | |
| 2.9.2 | 'comment' | comment to | textarea (text field) |
| | (data field) | the selected | |
| | | type | |

| Data block (field) No. | ldentifier of data block (field) | Content of data block (field) | Data field format | E-mail format | Obligation of informing | Stages of information provision |
|---------------------------------|-------------------------------------|---|--|--|----------------------------|---------------------------------------|
| 3 | ʻsourceld' (data field) | identifier assigned by an information exchange participant | information exchange participant | 'socialEngineering': { | [N] | [2], [3] |
| 3.1 | 'soiTypes' (data field) | identifiers of social engineering methods | telephone number starting with 8-800; [SMS] – an SMS message; [SNW] – social engineering using social networks; [MSG] – social engineering using instant messaging tools; | 'phoneNumber': '1212312345678', 'email': 'qwerty@example.ru', 'server': '127.0.0.1' }], 'messageAttachment': { 'sourceld': 'f34030ef-358a- 445c-8567-25985ce6d91c', 'comment': 'comment to the attachment', 'comment': 'comment to the attachment', 'dateTimeAt': '2018-03- 22T08:14:38Z', 'file': { 'name': 'file name', 'size': 'file size in bytes', 'base64': 'attachment in base64 format' }, 'fileLink': 'http://domain.com/archive.rar ' | [N] | [2], [3] |
| 3.2 | 'soiSenders' (data block) | social engineering implementati on identifiers | If it is necessary to specify several data field values (phoneNumber, email, server), specify one or several objects in the data block 'soiSenders' | }, 'description': 'additional description' }, | [N] | [2], [3] |

6.6.3. Computer attacks that have been launched as a result of inducing clients to conduct money transfer transactions through deception or abuse of trust **[socialEngineering]** (for [EXT] vector)

| 3.2.1 | 'phoneNumber' (data field) | telephone number | in the KKKXXXNNNNNNN format, where: KKK – a country code of one to three characters; XXX – operator's code; NNNNNNN - seven characters of the number. The telephone number is to be provided without a plus sign (+), spaces (_) and separation signs (-). |
|-------|---|---|--|
| 3.2.2 | ʻemail' (data field) | | The sender's e-mail address shall be submitted in the format in accordance with Specification RFC 5322 [18] |
| 3.2.3 | 'server' (data field) | IP address of the last mail server | Logical IPv4 address shall comply with Specification RFC 791 [12] |
| 3.3 | 'message Attach- ment' (data block) | data files describing the social engineering method | |
| 3.3.1 | ʻsourceld' (data field) | identifier assigned by an information exchange participant | 128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by an information exchange participant |
| 3.3.2 | 'comment' (data field) | description of the attachment | textarea (text field) |
| 3.3.3 | 'dateTimeAt' | | data provision format |

| | (data field) | | in accordance with |
|---------|-----------------|----------------|-----------------------------|
| | | was added | Specification RFC 3339 |
| | | | [11] |
| 3.3.4.1 | 'file' | data files | Specify the name and size |
| | (data subblock) | describing the | of the file (no more than 5 |
| | | social | MB) and perform Base64 |
| | | engineering | encoding |
| | | method | |
| 3.3.5 | 'fileLink' | data files | Specify URL for |
| | (data field) | describing the | downloading the file, if |
| | | social | its size exceeds 5 MB, in |
| | | engineering | accordance with |
| | | method | Specification RFC 3986 |
| | | | [15] |
| 3.4 | 'description' | additional | textarea (text field) |
| | (data field) | description | |

6.6.4. Denial of service computer attacks (DDoS attacks) in relation to the information infrastructure of information exchange participants [ddosAttacks] (for [INT] vector)

| Data block (field) No. | ldentifier of data block (field) | Content of data block (field) | Data field format | E-mail format | Obligation of informing | Stages of information provision |
|---------------------------------|-------------------------------------|---|---|--|----------------------------|---------------------------------------|
| 4 | ʻsourceld' (data field) | identifier assigned by an information exchange participant | 128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by an information exchange participant | 'ddosAttacks': [{ | [N] | [2], [3] |
| 4.1 | 'target' (data block) | attacked object identifiers | | 'url': 'http://example.com', 'assignment': 'purpose of the object under attack', | [N] | [2], [3] |
| 4.1.1 | 'ip' (data field) | IP address | Logical IPv4 address shall comply with Specification RFC 791 [12] | 'serviceType': 'information service type', 'network': 'network address' }, | [N] | [2], [3] |
| 4.1.2 | 'domain' (data field) | domain name | Domain name as per Specification RFC 1034 [14], as well as the international hierarchy of domain zones as per Specification RFC 5890 [13] | 'attackType': { 'type': 'attack type (by OSI levels)', - - ćcomment': 'additional description' | [N] | [2], [3] |

| 4.1.3 4.1.4 4.1.5 4.1.6 | 'url' (data field) 'assignment' (data field) 'serviceTyp' (data field) 'network' (data field) | URL-address URL-address purpose of the attacked object information service type network address | object in the information infrastructure of an information exchange participant (server, data storage system, telecom, personal computer, firewall, etc.) textarea Logical IPv4 address in accordance with Specification RFC 791 [12] specifying the network | <pre>}], 'po per second', per second,' per 'sta 221 second' 03- 'ne }], </pre> | urces': [{ | [N] [N] [N] | [2], [3] [2], [3] [2], [3] |
|----------------------------------|--|---|---|--|------------|-------------------|----------------------------------|
| 4.2 | 'attackType' | attack type | accordance with Specification RFC 997 [17] [17] | | | | |
| | (data block) | | | | | [N] | [2], [3] |
| 4.2.1 | 'type' (data field) | type of attack (by OSI levels) | One code shall be selected from the limited set of possible values: [1] – 'L2/3: ICMP-flood', [2] – 'L2/3: NTP- amplification', [3] – 'L2/3: TFTP- amplification', [4] – 'L2/3: SENTINEL- | | | [N] | [2], [3] |

| amplification', | |
|--|--|
| [5] – 'L2/3: DNS- | |
| amplification', | |
| [6] – 'L2/3: SNMP- amplification', | |
| [7] – 'L2/3: SSDP- amplification', | |
| [8] – 'L2/3: CHARGEN- amplification', | |
| [9] – 'L2/3: RIPv1- amplification', | |
| [10] – 'L2/3: BitTorrent- amplification', | |
| [11] – 'L2/3: QTPD- amplification', | |
| [12] – 'L2/3: Quake- amplification', | |
| [13] – 'L2/3: LDAP- amplification', | |
| [14] – 'L2/3: 49ad34- amplification', | |
| [15] – 'L2/3: Portmap- amplification', | |
| [16] – 'L2/3: Kad- amplification', | |
| [17] – 'L2/3: NetBIOS- amplification', | |
| [18] – 'L2/3: Steam- amplification', | |
| [19] – 'L3: DPI-attack', | |
| [20] – 'L4: LAND-attack', | |
| [21] – 'L4: TCP- SYN- attack', | |
| [22] – 'L4: TCP-ACK- | |

STO BR BFBO-1.5-

| | | | attack' |
|-------|---------------------------|-------------------------------|--|
| | | | attack', |
| | | | [23] – 'L4: Smurf-attack', |
| | | | [24] – 'L4: ICMP/UDP- frag', |
| | | | [25] – 'L4: TCP-frag', |
| | | | [26] – 'L6: SSL-attack', |
| | | | [27] – 'L7: DNS Water Tor- ture Attack', |
| | | | [28] – 'L7: Wordpress Pingback DDoS', |
| | | | [29] – 'L7: DNS-flood', |
| | | | [30] – 'L7: HTTP/S-flood', |
| | | | [31] – 'L7: FTP-flood', |
| | | | [32] – 'L7: SMTP-flood', |
| | | | [33] – 'L7: VoIP/SIP- attack', |
| | | | [34] – 'L7: POP3-flood', |
| | | | [35] – 'L7: SlowRate- attack,' |
| | | | [36] – 'other' |
| 4.2.2 | 'comment' | additional | textarea (text field) |
| 4.3 | (data field) 'sources' | description identification | If it is necessary to specify |
| | (data block) | of attack | several values of the data |
| | | sources | field (ip), specify one or |
| | | | several objects in the data block 'sources' |
| | | | |
| 4.3.1 | 'ip' | | Logical IPv4 address |
| | (data field) | the attack source (in | shall comply with Specification RFC 791 |
| | | case of a large | |
| | | number of | |
| | | computer attack sources | |
| | | in the | |
| | | block | |

| | | - specify the top 100 IP | |
|--------|-------------------------------|-------------------------------------|---|
| | | addresses of the attackers, | |
| | | with the complete list | |
| | | attached in a text file) | |
| 4.4 | 'power' (data block) | attack power | |
| 4.4.1 | 'pps' (data field) | number of packets per second | Packets per second |
| 4.4.2 | 'mps' (data field) | number of megabits per second | Megabits per second |
| 4.4.3 | 'rps' (data field) | number of requests per second | Requests per second |
| 4.5 | 'startTimeAt' (data field) | attack start time | data provision format in accordance with Specification RFC 3339 [11] |
| 4.6 | 'end time' (data field) | attack end time | data provision format in accordance with Specification RFC 3339 |
| 4.7 | 'negativeImpact' | attack | [11] |
| 4.7 | (data block) | negative impact | |
| 4.7.1. | 'type' (data field) | negative impact type | One code shall be selected from the limited |
| | | | set of possible values:[NAW] – service |
| | | | availability interruption;[OTH] – service |
| | | | degradation; |

| [NCQ] – service was not adversely affected | |
|--|-----|
| nt' additional textarea (text field) ld) description | [N] |

6.6.5. Computer attacks related to unauthorised access to ATMs and payment terminals of information exchange participants **[atmAttacks]** (for vector [INT])

| Data block (field) No. | ldentifier of data block (field) | Content of data block (field) | Data field format | E-mail format | Obligation of informing | Stages of information provision |
|---------------------------------|-------------------------------------|---|---|---|----------------------------|---------------------------------------|
| 5 | ʻsourceld' (data field) | identifier assigned by an information exchange participant | 128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by an information exchange participant | 'atmAttacks': { | [N] | [2], [3] |
| 5.1 | 'target' (data block) | identifier of the attacked object | | description' }, 'attackType': [{ 'type': attack type depending | [N] | [2], [3] |
| 5.1.1 | ʻtype' (data field) | attacked object type | • [OTH] is other facility | on the target description' }], 'attackImage': { 'sourceld': 'f34030ef-358a- 445c-8567-25985ce6d91c', 'comment': 'comment to the attachment', 22T08:14:38Z', 'file': { 'name': 'file name', 'size': 'file size in bytes', 'base64': 'attachment | [N] | [2], [3] |
| 5.1.2 | 'description' (data field) | additional description | textarea (text field) | in base64 format' }, | [N] | [2], [3] |

| 5.2 | 'attackType' (data block) | attack type | If it is necessary to specify several values of data fields (type, description), specify one or several | 'http://domain.com/archive.r ar ' } | [N] | [2], [3] |
|---------|-------------------------------|---|--|---|-----|----------|
| | | | objects in the data block 'sources' | }, | | |
| 5.2.1 | ʻtype' (data field) | type of attack depending on the target | One code shall be selected from the limited set of possible values: • [BBX] – blackbox attacks; • [DSP] – direct dispense attacks and their variations; • [SKM] – skimming; • [OTH] – other method | | [N] | [2], [3] |
| 5.2.2 | 'description' (data field) | additional description | textarea (text field) | | [N] | [2], [3] |
| 5.3 | 'attackImage' (data block) | additional materials of attack events | | | [N] | [2], [3] |
| 5.3.1 | ʻsourceld' (data field) | identifier assigned by an information exchange participant | 128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by an information exchange participant | | [N] | [2], [3] |
| 5.3.2 | (data field) | description of the attachment | textarea (text field) | | [N] | [2], [3] |
| 5.3.3 | 'dateTimeAt' (data field) | date and time | data provision format in accordance with Specification RFC 3339 [11] | | [N] | [2], [3] |
| 5.3.4.1 | 'file' (data subblock) | data file containing additional materials | Specify the name and size of the file (no more than 5 MB) and perform Base64 encoding | | [N] | [2], [3] |

| 5.3.5 | 'fileLink' | | Specify the URL-address |
|-------|--------------|--------------|----------------------------|
| | (data field) | | for downloading a file, if |
| | | (downloading | its size exceeds 5 MB, in |
| | | | accordance with |
| | | containing | Specification RFC 3986 |
| | | additional | [15] |
| | | materials | |
| | | | |

6.6.6. Computer attacks related to exploiting information infrastructure vulnerabilities of information exchange participants and their clients **[vulnerabilities]** (for vector [INT], [EXT])

| Data block (field) No. | ldentifier of data block (field) | Content of data block (field) | Data field format | E-mail format | Obligation of informing | Stages of information provision |
|---------------------------------|-------------------------------------|---|--|---|----------------------------|---------------------------------------|
| 6 | ʻsourceld' (data field) | identifier assigned by an information exchange participant | 128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by an information exchange participant | 'vulnerabilities': [{ | [N] | [2], [3] |
| 6.1 | 'target' (data block) | attacked object identifiers | | <pre>'example.com', 'url':</pre> | [N] | [2], [3] |
| 6.1.1 | 'ip' (data field) | IP address | Logical IPv4 address shall comply with Specification RFC 791 [12] | service type', }, 'sources': [{ 'ip': '127.0.0.1', 'url': 'http://example.com' | [N] | [2], [3] |
| 6.1.2 | 'domain' (data field) | domain name | Domain name according to Specification RFC 1034 [14] and the international hierarchy of domain zones according to Specification RFC 5890 [13] | | [N] | [2], [3] |
| 6.1.3 | 'url' (data field) | URL-address | URL in accordance with Specification RFC 3986 [15] | 'swName': 'software name'. программного обеспечения', 'swVer': 'software version', 'cweType': 'CWE error type', | [N] | [2], [3] |

| 6.1.4 | 'serviceType' (data field) | type of information service | textarea (text field) | 'class': 'vulnerability class', 'osName': 'operating system that controls software with detected vulnerabilities', 'detectedAt': date and time | [N] | [2], [3] |
|-------|-------------------------------|-----------------------------------|---|--|-----|----------|
| 6.2 | 'sources' (data block) | | If it is necessary to specify several values of data fields (ip, url), specify one or several objects in the data block 'sources' | of vulnerability detection', 'baseCVSS': 'baseline vector of vulnerability', 'danger': 'severity level of detected vulnerability', 'measures': 'potential measures | [N] | [2], [3] |
| 6.2.1 | 'ip' (data field) | IP address | Logical IPv4 address shall comply with Specification RFC 791 [12] | to eliminate vulnerability', 'status': 'vulnerability status', 'exploit': 'exploit availability', 'recommendation': | [N] | [2], [3] |
| 6.2.2 | 'url' (data field) | URL-address | URL in accordance with Specification RFC 3986 [15] | 'information on vulnerability elimination', 'link': 'links to sources of | [N] | [2], [3] |
| 6.3 | 'identifier' (data field) | vulnerability identifier | If a vulnerability is detected, its type is to be specified in accordance with the classification of the FSTEC of Russia - https://bdu.fstec.ru/ vul; • Common Vulnerabilities and Exposures (CVE), https://cve.mitre.org/dat a/d ownloads/allitems.html | | [N] | [2], [3] |
| 6.4 | 'cvss' (data field) | CVSS metrics | Specify CVSS v 3.0 Metrics (the Common Vulnerability Scoring System (CVSS) if * is defined. Specify the maximum possible number of metrics listed as follows: basic metrics, temporary metrics, context metrics, and environment metrics. (* If no metrics are defined, | | [N] | [2], [3] |

STO BR BFBO-1.5-

| | | use the FSTEC of Russia |
|---------------|--|--|
| | | calculator |
| | | https://bdu.fstec.ru/cvss3 |
| | |) |
| | | |
| (data block) | | |
| | lacitation | |
| 'description' | vulnerability | textarea (text field) |
| | | |
| | | textarea (text field) |
| (untu nelu) | | |
| 'swVer' | software | textarea (text field) |
| (data field) | version | |
| 'sweType' | type of error | in accordance with |
| | | Common Weakness |
| . , | accordance | Enumeration (CWE) |
| | | (https://cwe.mitre.org/) |
| | | |
| | CWL enois | |
| 'class' | vulnerability | One code shall be |
| (data field) | class | selected from the limited |
| | | set of possible values: |
| | | [COD] – code vulnerability - a |
| | | vulnerability resulting |
| | | from software |
| | | development, excluding |
| | | data security |
| | | requirements; • [ARH] – |
| | | • [ARH] – architecture |
| | | vulnerability - a |
| | | vulnerability resulting |
| | | from the choice and |
| | | composition of software components containing |
| | | vulnerabilities; |
| | (data field) 'swName' (data field) 'swVer' (data field) 'sweType' (data field) | (data block)vulnerability identifier'description'vulnerability identifier'description'vulnerability description'swName'software name(data field)software version'swVer'software version'sweType'type of error established in accordance with the general list of CWE errors'class'vulnerability |

| | | | • [MULT] – multiple- |
|--------|--------------|------------------------|---|
| | | | factor vulnerability |
| | | | (caused by various |
| | | | classes of vulnerabilities in the software) |
| | | | In the software) |
| | | | |
| 6.5.6 | 'osName' | an operating | Textarea (text field) |
| | (data field) | system that | |
| | | controls | |
| | | software with detected | |
| | | vulnerabilities | |
| | | | |
| | | | |
| | | | |
| | | | |
| 6.5.7 | 'dateTimeAt' | date and time when | data provision format in accordance with |
| | (data field) | - | Specification RFC 3339 |
| | | was detected | |
| 6.5.8 | 'baseCVSS' | baseline | in accordance with CVSS |
| | (data field) | vulnerability | 3.0 |
| | | vector | (https://bdu.fstec.ru/cvss3 |
| 6.5.9 | 'danger' | severity level | One code is to be |
| 0.5.9 | (data field) | of identified | selected from the limited |
| | (data neid) | vulnerability | set of possible values in |
| | | vanerability | accordance with the |
| | | | results of the baseline |
| | | | vulnerability vector: |
| | | | • [LL] – low level, if |
| | | | 0.0 < = V < = 3.9; |
| | | | • [ML] – mean level, |
| | | | if 4.0 < = V < = 6.9; |
| | | | • [HL] – high level, if |
| | | | 7.0 < = V < = 9.9; |
| | | | • [CL] – critical |
| | | | level, if V = 10.0 |
| 6.5.10 | 'measures' | possible | textarea (text field) |
| | (data field) | measures to | |

| | | eliminate | |
|---------|------------------------|----------------------------|--|
| | | vulnerability | |
| 6.5.11 | 'status' | vulnerability | One code shall be selected |
| 0.0.11 | (data field) | status | from the limited set of |
| | (| | possible values: |
| | | | • [APR_M] - |
| | | | confirmed by the |
| | | | manufacturer' |
| | | | if a vulnerability was |
| | | | confirmed by the |
| | | | manufacturer (developer) |
| | | | of software containing a |
| | | | vulnerability; |
| | | | • [APR_M] – |
| | | | 'confirmed in the course |
| | | | of research' - if a |
| | | | vulnerability was |
| | | | detected and confirmed |
| | | | by a researcher |
| | | | (organisation) who is not |
| | | | the software |
| | | | manufacturer |
| | | | (developer); |
| | | | • [Potential] – |
| | | | 'potential vulnerability' – |
| | | | in all other cases |
| 6.5.12 | 'exploit' | existence of | Textarea (text field) |
| | (data field) | exploit | |
| 6.5.13 | 'recommendation | | Textarea (text field) |
| | (data field) | on the | |
| | | elimination of | |
| 6 5 4 4 | llin I.I. (det e | vulnerability reference | T |
| 6.5.14 | 'link' (data field) | links to | Textarea (text field) |
| | neid) | sources of | |
| | | information | |
| | | on the | |
| | | elimination of | |
| | | vulnerability | |
| 6.5.15 | 'manufacturer' | a company | Textarea (text field) |
| | (data field) | (organisation) | |
| | | that is the | |
| | | manufacturer | |
| | | (developer | |

| of software | | |
|---------------|--|--|
| in which a | | |
| vulnerability | | |
| has been | | |
| detected | | |
| | | |

6.6.7. Computer attacks related to searching (hacking) and compromising authentication data (login) data

[bruteForces] (for [INT] vector)

| Dete | | | | | | |
|---------------------------------|-------------------------------------|---|--|---|----------------------------|---------------------------------------|
| Data block (field) No. | ldentifier of data block (field) | Content of data block (field) | Data field format | E-mail format | Obligation of informing | Stages of information provision |
| 7 | ʻsourceld' (data field) | identifier assigned by an information exchange participant | 128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by an information exchange participant | 'bruteForces': [{ 'sourceld': 'f34030ef-358a-445c- 8567- 25985ce6d91c', 'target': { 'ip': '127.0.0.1', 'url': | [N] | [2], [3] |
| 7.1 | 'target' (data block) | attacked object attacked object | | 'http://example.com', 'serviceType': 'service type' }, | [N] | [2], [3] |
| 7.1.1 | 'ip' (data field) | IP address | Logical IPv4 address shall comply with Specification RFC 791 [12] | 'sources': [{ 'ip': '127.0.0.1' }], 'accountOs': { | [N] | [2], [3] |
| 7.1.2 | 'domain' (data field) | domain name | Domain name according to Specification RFC 1034 [14] and the international hierarchy of domain zones according to Specification RFC 5890 [13] | 'name': 'account name', 'privileges': 'account (privilege) | [N] | [2], [3] |
| 7.1.3 | 'url' (data field) | URL-address | URL in accordance with Specification RFC 3986 [15] | | [N] | [2], [3] |
| 7.1.4 | 'serviceTyp' (data field) | type of information service | Textarea (text field) | | [N] | [2], [3] |
| 7.2 | 'sources' (data block) | identifiers of attack source | If it is necessary to specify several values of the data field (ip), specify one or several objects in the data block 'sources' | | [N] | [2], [3] |

| 'ip' (data field) IP address of the source of attack (in the case of a large number of computer attack sources, the sources data block shall contain the top 100 IP addresses of the attackers with the complete list attached in a text file) | [N] |
|--|-----|
| 'accountOs' compromise (data block) d account identiriers | [N] |
| 'name'accountTextarea (text field)(data field)name | [N] |
| 'privileges'account levelTextarea (text field)(data field)(privileges) | [N] |

| 6.6.8. Computer attacks related to spam mailings to information exchange participants and their clients [spams] |
|---|
| (for [INT], [EXT] vector) |

| Data block (field) No. | ldentifier of data block (field) | Content of data block (field) | Data field format | E-mail format | Obligation of informing | Stages of information provision |
|---------------------------------|-------------------------------------|---|--|--|-------------------------|---------------------------------------|
| 8 | ʻsourceld' (data field) | identifier assigned by an information exchange participant | 128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by an information exchange participant | 'spams': [{ 'sourceld': 'f34030ef-358a-445c- 8567- 25985ce6d91c', 'receivedAt': '2018-03 22T08:14:38Z', 'targets': [{ 'email': 'gwerty@example.ru' | [N] | [2], [3] |
| 8.1 | 'receivedAt' (data field) | date and time when a spam message is received | data provision format in accordance with Specification RFC 3339 [11] | }], 'sources': [{ 'ip': '127.0.0.1', 'domain': 'example.com', 'email': 'qwerty@example.ru' | [N] | [2], [3] |
| 8.2 | 'target' (data block) | attacked object identifiers (recipients of spam messages) | If it is necessary to specify several values of the data field (email), specify one or several objects in the 'targets' data block | <pre>}],</pre> | [N] | [2], [3] |
| 8.2.1 | ʻemail' (data field) | spam message recipient's email address | The sender's e-mail address shall be submitted in the format in accordance with Specification RFC 5322 [18] | 'dateTimeAt': '2018-03- 22T08:14:38Z ', 'file': { 'name': 'file name', 'size': 'file size in bytes', | [N] | [2], [3] |
| 8.3 | 'sources' (data block) | attack source identifiers (spam sender) | If it is necessary to specify several data field values (ip, domain, email), specify one or several objects in the data block 'sources' | 'base64': 'attachment in in base64 format' }, 'fileLink': 'http://domain.com/archive.rar' } | [N] | [2], [3] |
| 8.3.1 | 'ip' (data field) | IP address | Logical IPv4 address shall comply with Specification RFC 791 [12] | }], | [N] | [2], [3] |

| 8.3.2 | 'domain' (data field) | domain name | Domain name according to Specification RFC 1034 [14] and the international hierarchy of domain zones according to Specification RFC 5890 [13] |
|---------|------------------------------|---|--|
| 8.3.3 | ʻemail' (data field) | sender's e- mail address | The sender's e-mail address shall be submitted in the format in accordance with Specification RFC 5322 [18] |
| 8.4 | 'spamImage' (data block) | spam message example | |
| 8.4.1 | ʻsourceld' (data field) | identifier assigned by an information exchange participant | 128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by an information exchange participant |
| 8.4.2 | | description of the attachment | Textarea (text field) |
| 8.4.3 | 'dateTimeAt' (data field) | date and time when the file was added | data provision format in accordance with Specification RFC 3339 [11] |
| 8.4.4.1 | 'file' (data block) | data file containing additional materials | Specify the name and size of the file (no more than 5 MB) and perform Base64 encoding |
| 8.4.5 | 'fileLink' (data field) | for obtaining | Specify the URL-address for downloading a file, if its size exceeds 5 MB, in accordance with Specification RFC 3986 [15] |

| Data block (field) No. | ldentifier of data block (field) | Content of data block (field) | Data field format | E-mail format | Obligation of informing | Stages of information provision |
|---------------------------------|-------------------------------------|--|---|---|----------------------------|---------------------------------------|
| 9 | ʻsourceld' (data field) | identifier assigned by an information exchange participant | 128-bit identifier (GUID) generated in accordance with RFC specification 4122 [16] assigned by an information exchange participant | 'controlCenters': [{ 'sourceld': 'f34030ef-358a-445c- 8567- 25985ce6d91c', 'target': { 'ip': '127.0.0.1', 'url': 'http://example.com' | [N] | [2], [3] |
| 9.1 | 'target' (data block) | attacked object identifiers | | }, 'hostUrl': 'http://example.com', 'intruderIp': '1.1.1.1', | [N] | [2], [3] |
| 9.1.1 | 'ip' (data field) | IP address | Logical IPv4 address shall comply with Specification RFC 791 [12] | 'intruderActions': 'what preceded | [N] | [2], [3] |
| 9.1.2 | 'url' (data field) | URL-address | URL in accordance with Specification RFC 3986 [15] | the Botnet Command Centre', 'nodes': [{ 'ip': '127.0.0.1', | [N] | [2], [3] |
| 9.2 | 'hostUrl' (data field) | URL hosting the Botnet Command Centre | URL in accordance with Specification RFC 3986 [15] | 'lastRequestRateTimeAt': '2018- 03-22T08:08:49Z' }] }], | [N] | [2], [3] |
| 9.3 | 'intruderlp' (data field) | the attacker | Logical IPv4 address shall comply with Specification RFC 791 [12] | | [N] | [2], [3] |
| 9.4 | 'intruderActions' (data field) | description of unauthorised activity in the information infrastructur e of an information | Textarea (text field) | | [N] | [2], [3] |

6.6.9. Computer attacks related to detecting an interaction of information infrastructure facilities of information exchange participants with Botnet command centres **[controlCenters]** (for [INT] vector)

| | | avela e a a a | |
|-------|---|--|--|
| | | exchange participant | |
| | | participant | |
| 9.5 | 'description' (data field) | additional description of the Botnet command centre | Textarea (text field) |
| 9.6 | 'nodes' (data block) | identifiers of appeals to the Botnet command centre | If it is necessary to specify several data field values (ip, lastRequestRateTimeAt), specify one or several objects in the data block |
| 9.6.1 | 'ip' (data field) | external IP address (information exchange participant) | Logical IPv4 address shall comply with Specification RFC 791 [12] |
| 9.6.2 | 'lastRequest RatetimeAt' (data field) | date and time of the last interaction with the Botnet command centre | data provision format in accordance with Specification RFC 3339 [11] |

6.6.10. Computer attacks related to the change (substitution) of the mobile subscriber identifier (IMSI) of the SIM card number,

as well as the replacement of the mobile equipment identifier (IMEI) [sim] (for [EXT] vector)

| Data block (field) No. | ldentifier of data block (field) | Content of data block (field) | Data field format | E-mail format | Obligation of informing | Stages of information provision |
|---------------------------------|-------------------------------------|---|---|--|----------------------------|---------------------------------------|
| 10 | 'sourceld' (data field) | identifier assigned by an information exchange participant | 128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by an information exchange participant | 'sim': { | [N] | [2], [3] |
| 10.1 | 'mobileOperator' | name of a | Textarea (text field) | 'imsi': '123456789000000', 'imsiChangedAt': '2018-03- | [N] | [2], [3] |

| | (data field) | mobile operator | | 22T08:08:49Z' }, | | |
|------|---------------------------------|--|---|---------------------|-----|----------|
| 10.2 | 'phoneNumber' (data field) | mobile phone number | in the KKKXXXNNNNNNN format, where: KKK – a country code of one to three characters; XXX – operator's code; NNNNNNN – seven characters of the number. The telephone number is to be provided without a plus sign (+), spaces (_) and separation signs (-). | | [N] | [2], [3] |
| 10.3 | 'imsi' (data field) | unique SIM card number (IMSI number) | in the XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX | | [N] | [2], [3] |
| 10.4 | 'imsiChangedAt' (data field) | when the IMSI | data provision format in accordance with Specification RFC 3339 [11] | | [N] | [2], [3] |

6.6.11. Computer attacks related to information that misleads information exchange participants and their clients, as well as other persons interacting with them, about the ownership of the information disseminated via the Internet due to the similarity of domain names, design or content. Phishing [phishingAttacks] (for [EXT], [INT] vector)

| Data block (field) No. | ldentifier of data block (field) | Content of data block (field) | Data field format | E-mail format | Obligation of informing | Stages of information provision |
|---------------------------------|-------------------------------------|---|--|--|----------------------------|---------------------------------------|
| 11 | ʻsourceld' (data field) | identifier assigned by an information exchange participant | 128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by an information exchange | 'phishingAttacks': [{ 'sourceld': 'f34030ef-358a-445c- 8567- 25985ce6d91c', 'target': { 'ip': '127.0.0.1', 'domain': 'example.com' | [N] | [2], [3] |

| | | | participant | | }, | | |
|--------|---|---|--|--|--|-----|----------|
| 11.1 | 'target' (data block) | identifier of the attacked object (legitimate resourse) | | | <pre>''harmful': [{</pre> | [N] | [2], [3] |
| 11.1.1 | 'ip' (data field) | IP address | Logical IPv4 address shall comply with Specification RFC 791 [12] | 445c-8567-25985ce6d91c', | <pre>'messageAttachment': {</pre> | [N] | [2], [3] |
| 11.1.2 | 'domain' (data field) | domain name | Domain name according to Specification RFC 1034 [14], as well as the international hierarchy of domain zones according to Specification RFC 5890 [13] | 22T08:08:49Z', 'http://domain.com/archive.r | description' dateTimeAt': '2018-03- 'file': { 'name': 'file name', 'size': 'file size in | [N] | [2], [3] |
| 11.2 | 'harmful' (data block) | phishing resource source identifiers | If it is necessary to specify several values of data fields (ip, url), specify one or several objects in the data block 'harmful' | ar' }], | bytes' 'base64': 'attachment in base64 format' | [N] | [2], [3] |
| 11.2.1 | ʻip' (data field) | IP address | Logical IPv4 address shall comply with Specification RFC 791 [12] | | }, 'fileLink': } | [N] | [2], [3] |
| 11.2.2 | ʻurl' (data field) | URL-address | URL in accordance with Specification RFC 3986 [15] | | | [N] | [2], [3] |
| 11.3 | ʻfixationAt' (data field) | date and time of phishing message recording | | | | [N] | [2], [3] |
| 11.4 | 'message Attachment' (data block) | phishing message sample | | | | [N] | [2], [3] |
| 11.4.1 | 'sourceld' (data field) | identifier assigned by an information | 128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by | | | [N] | [2], [3] |

| | | exchange participant | an information exchange participant |
|--------------|------------------------------|--|--|
| 11.4.2 | (data field) | description of the attachment | Textarea (text field) |
| 11.4.3 | 'dateTimeAt' (data field) | | data provision format in accordance with Specification RFC 3339 [11] |
| 11.4.4. 1 | 'file' (data block) | data file containing additional materials | Specify the name and size of the file (no more than 5 MB) and perform encoding in Base64 formate |
| 11.4.5 | 'fileLink' (data field) | for obtaining | Specify the URL-address for downloading a file, if its size exceeds 5 MB, in accordance with RFC Specification 3986 [15] |

6.6.12. Computer attacks related to the distribution of information related to offers and/or provision of financial services in the Russian Federation by persons not entitled to provide them in accordance with the legislation of the Russian Federation. Posting prohibited content on the Internet **[prohibitedContents]**(for [EXT], [INT] vector)

| | Data block (field) lo. | ldentifier of data block (field) | Content of data block (field) | Data field format | E-mail format | Obligation of informing | Stages of information provision |
|---|---------------------------------|-------------------------------------|---|---|---|----------------------------|---------------------------------------|
| 1 | 2 | ʻsourceld' (data field) | identifier assigned by an information exchange participant | 128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by an information exchange participant | 'prohibitedContents': [{ 'sourceld': 'f34030ef-358a-445c- 8567- 25985ce6d91c', 'sources': [{ 'ip': '127.0.0.1', 'url': 'http://example.com' | [N] | [2], [3] |
| 1 | 2.1 | 'sources' (data block) | identifiers of prohibited content sources | If it is necessary to specify several values of data fields (ip, url), specify one or several objects in the 'target' data block | }], 'type': 'prohibited content type' }], | [N] | [2], [3] |

| 12.1.1 | 'ip' (data field) | IP address | Logical IPv4 address shall comply with Specification RFC 791 [12] |
|--------|------------------------|----------------------------|---|
| 12.1.2 | 'url' (data field) | URL-address | URL in accordance with Specification RFC 3986 [15] |
| 12.2 | 'type' (data field) | prohibited content type | textarea (text field) |

6.6.13. Computer attacks related to posting on the Internet information enabling illegal access to information systems of information exchange participants and their customers used for providing (receiving) financial services, including through illegal access to confidential customer information. Posting a malicious resource on the Internet **[maliciousResources]** (for [EXT], [INT] vector)

| Data block (field) No. | ldentifier of data block (field) | Content of data block (field) | Data field format | E-mail format | Mandatory provision of information | Information provision stages |
|---------------------------------|--|---|---|-------------------------------------|---|------------------------------------|
| 13 | 'sourceld' (data field) | identifier assigned by an information exchange participant | 128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by an information exchange participant | <pre>'maliciousResources': [{</pre> | [N] | [2], [3] |
| 13.1 | ʻsources' (data block) | identifiers of malicious resource sources | If it is necessary to specify several values of data fields (ip, url), specify one or several objects in the 'target' data block | | [N] | [2], [3] |
| 13.1.1 | 'ip' (data field) | IP address | Logical IPv4 address shall comply with Specification RFC 791 [12] | | [N] | [2], [3] |
| 13.1.2 | 'url' | URL-address | URL in accordance with | | [N] | [2], [3] |

| | (data field) | | Specification RFC 3986 [15] |
|------|--------------------------------|----------------------|--------------------------------|
| 13.2 | 'activityType' (data field) | type of malicious | textarea (text field) |
| | (data neid) | activity | |

6.6.14. Computer attacks related to changes in content [changeContent] (for [INT] vector)

| Data block (field) No. | ldentifier of data block (field) | Content of data block (field) | Data field format | E-mail format | Obligation of informing | Stages of information provision |
|---------------------------------|-------------------------------------|---|---|--------------------------------|----------------------------|---------------------------------------|
| 14 | ʻsourceld' (data field) | identifier assigned by an information exchange participant | 128-bit identifier (GUID) generated in accordance with RFC specification 4122 [16] assigned by an information exchange participant | <pre>'changeContent': [{</pre> | [N] | [2], [3] |
| 14.1 | 'targets' (data block) | attacked objects which | If it is necessary to specify several values of data fields (ip, url), specify one or several objects in the 'target' data block | | [N] | [2], [3] |
| 14.1.1 | 'ip' (data field) | IP address | Logical IPv4 address shall comply with Specification RFC 791 [12] | | [N] | [2], [3] |
| 14.1.2 | 'url' (data field) | URL-address | URL in accordance with Specification RFC 3986 [15] | | [N] | [2], [3] |
| 14.2 | 'type' (data field) | type of modified content | textarea (text field) | | [N] | [2], [3] |

STO BR BFBO-1.5-
6.6.15. Computer attacks related to the scanning of software ports of information infrastructure facilities of information exchange participants by persons not authorised to do so **[scanPorts]** (for [INT] vector)

| Data block (field) No. | ldentifier of data block (field) | Content of data block (field) | Data field format | E-mail format | Obligation of informing | Stages of information provision |
|---------------------------------|-------------------------------------|--|---|---|----------------------------|---------------------------------------|
| 15 | ʻsourceld' (data field) | identifier assigned by an information exchange participant | 128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by an information exchange participant | 'scanPorts': [{ | [N] | [2], [3] |
| 15.2 | 'sources' (data block) | malicious activity source identifiers | If it is necessary to specify several values of the data field (email), specify one or several objects in the 'sources' data block | 'ports': ['21'], 'method': 'information on scanning methods or software used for this purpose', 'startTimeAt': '2018-03- 22T08:08:49Z', 'endTimeAt': '2018- 03-22T08:09:49Z' | [N] | [2], [3] |
| 15.2.1 | 'ip' (data field) | IP address | Logical IPv4 address shall comply with Specification RFC 791 [12] | }], | [N] | [2], [3] |
| 15.3 | 'ports' (data field) | port numbers that have been scanned | textarea (text field) | | [N] | [2], [3] |
| 15.4 | 'method' (data field) | information on scanning methods or software used for this purpose | textarea (text field) | | [N] | [2], [3] |
| 15.5 | 'startTimeAt' (data field) | scanning start time | data provision format in accordance with Specification RFC 3339 [11] | | [N] | [2], [3] |

| 15.6 | 'end time' (data field) | scanning end time | data provision format in accordance with Specification RFC 3339 [11] | | [N] | [2], [3] |
|------|----------------------------|----------------------|---|--|-----|----------|
|------|----------------------------|----------------------|---|--|-----|----------|

6.6.16. Other computer attacks against information infrastructure facilities of information exchange participants and their clients **[other]** (for [INT], [EXT] vector)

| Data block (field) No. | ldentifier of data block (field) | Content of data block (field) | Data field format | E-mail format | Obligation of informing | Stages of information provision |
|---------------------------------|-------------------------------------|---|---|--|----------------------------|---------------------------------------|
| 16 | ʻsourceld' (data field) | identifier assigned by an information exchange participant | 128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by an information exchange participant | 'other': { | [N] | [2], [3] |
| 16.1 | 'description' (data field) | computer attack attacked object | textarea (text field) | 'ip': '127.0.0.1', 'url': 'http://example.com' }, 'type': 'other type of prohibited, | [N] | [2], [3] |
| 16.2 | 'source' (data block) | identifiers of another source of malicious, prohibited content/ resource | | malicious, altered content', 'attachment': { 'sourceld': 'f34030ef-358a- 445c-8567-25985ce6d91c', description', 'dateTimeAt': '2018-03- | [N] | [2], [3] |
| 16.2.1 | 'ip' (data field) | IP address | Logical IPv4 address shall comply with Specification RFC 791 [12] | 22T08:08:49Z ', 'file': { 'name': 'file name', 'size': 'file size in bytes', | [N] | [2], [3] |
| 16.2.2 | 'url' (data field) | URL-address | URL in accordance with Specification RFC 3986 [15] | 'base64': 'attachment in base64 format' | [N] | [2], [3] |
| 16.2.3 | ʻtype' (data field) | other type of prohibited, malicious, modified content | textarea (text field) | }, 'fileLink': ' http://domain.com/archive.rar' } } } | [N] | [2], [3] |

STO BR BFBO-1.5-

| 16.3 | 'attachment' (data block) | additional data to identify a computer attack | |
|--------|------------------------------|---|--|
| 16.3.1 | ʻsourceld' (data field) | identifier assigned by an information exchange participant | 128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by an information exchange participant |
| 16.3.2 | 'comment' (data field) | attachment description | textarea (text field) |
| 16.3.3 | 'dateTimeAt' (data field) | date and time when the file was added | data provision format in accordance with Specification RFC 3339 [11] |
| 16.3.4 | 'file' (data block) | data file containing additional materials | Specify the name and size of the file (no more than 5 MB) and perform encoding in Base64 format |
| 16.3.5 | 'fileLink' (data field) | for obtaining | it is required to specify URL for downloading the file, if its size exceeds 5 MB, in accordance with Specification RFC 3986 [15] |

6.7. Information on the results of the completion of an incident and relevant forms of electronic messages

6.7.1. Organisational information [finalReport]

| Data block (field) No. | ldentifier of data block (field) | Content of data block (field) | Data field format | E-mail format | Obligation of informing | Stages of information provision |
|---------------------------------|-------------------------------------|---|---|---|----------------------------|---------------------------------------|
| 1.1 | 'closeDateAt' (data field) | date and time of incident closure | data provision format in accordance with Specification RFC 3339 [11] | 'finalReport': { | [0] | [3] |
| 1.2 | ʻrecovery' (data field) | identifier of recovery after incident occurrence | One code shall be selected from the limited set of possible values: • [Full] – provision of financial (banking) services is fully restored; • [Not_Full] – provision of financial (banking) services is partially restored | occurrence of the incident', 'description': 'additional description if recovery is impossible', 'rootCause': 'key causes of the incident', 'mainActions': 'actions taken to prevent incidents in the future', | [0] | [3] |
| 1.3 | 'description' (data field) | additional description if recovery is impossible | textarea (text field) | | [0] | [3] |
| 1.4 | ʻrootCause' (data field) | key causes of the incident | textarea (text field) | | [0] | [3] |
| 1.5 | 'mainActions' (data field) | actions taken to prevent future incidents | textarea (text field) | | [0] | [3] |

STO BR BFBO-1.5-

| Data block (field) No. | Data block (field) identifier | Content of data block (field) | Data field format | E-mail format | Mandatory provision of information | Information provision stages |
|---------------------------------|-------------------------------------|---|--|--|---|------------------------------------|
| 2.1 | ʻsignatures' (data block) | signature | If it is necessary to specify several data field values (identifier, name, source, eventsAmount), specify one or several objects in the data block 'signatures' | 'signatures': [{ 'identifier': 'signature identifier' - 'name': 'detection tool', 'source': 'signature source', 'eventsAmount': 'number of signature responses' | [N] | [3] |
| 2.2 | 'identifier' (data field) | unique identifier of the signature | sequence of symbols obtained as a result of MD5 hash function calculation | }], 'snort': ['rule1','rule2'], 'attachment': { 'sourceld': 'f34030ef-358a-445c- | [N] | [3] |
| 2.3 | 'name' (data field) | detection tool | textarea (text field) | 8567-25985ce6d91c', 'comment': 'description of the attachment', 'dateTimeAt': | [N] | [3] |
| 2.4 | 'source' (data field) | source of signature receipt | textarea (text field) | ʻ2018- 03- | [N] | [3] |
| 2.5 | 'eventsAmount' (data field) | number of signature responses | textarea (text field) | 22T08:14:38Z', 'file': { 'name': 'file name', 'size': 'file size in | [N] | [3] |
| 2.6 | ʻsnort' (data field) | Snort- rules | <pre>submission format in the form of: <action> <protocol> <sender ip<br="">addresses> <sender ports> <destination operator> <recipient IP addresses> <recipient ports=""> (key_1: value_1; key_2: value_2; key_n: value_n;)</recipient></recipient </destination </sender </sender></protocol></action></pre> | bytes', 'base64': 'attachment in base64 format' }, 'fileLink': 'http://domain.com/archive.rar' } } } | [N] | [3] |

6.7.2. Technical information describing the signature of computer attacks **[signatures]**

| 2.7 | 'attachment' (data block) | additional data upon completion of an incident | |
|-------|------------------------------|--|--|
| 2.7.1 | ʻsourceld' (data field) | identifier assigned by an informatio n exchange participant | 128-bit identifier (GUID) generated in accordance with RFC specification 4122 [16] assigned by an information exchange participant |
| 2.7.2 | 'comment' (data field) | attachment description | textarea (text field) |
| 2.7.3 | 'dateTimeAt' (data field) | date and time when the file was added | data provision format in accordance with Specification RFC 3339[11] |
| 2.7.4 | 'file' (data block) | data file containing additional materials | Specify the name and size of the file (no more than 5 MB) and perform Base64 encoding |
| 2.7.5 | 'fileLink' (data field) | link for obtaining (downloadi ng) a data file containing additional materials | Specify the URL for downloading the file, if its size exceeds 5 MB, in accordance with the RFC 3986 specification [15] |

STO BR BFBO-1.5-

If the Bank of Russia receives information in accordance with Chapter 6 of Section 6.5 hereof from an information exchange participant serving the payer in order to verify a particular payee, it shall send a request to the information exchange participant servicing the payee, as well as a notice of the suspension of the crediting of funds to the payee's bank account or an increase in the balance of the payee's electronic funds.

7.1. Identification data of the Bank of Russia's request. Data block [HEADER]

| Data block (field) No. | Data block (field) identifier | Data block (field) content | Data field format | E-mail format |
|---------------------------------|----------------------------------|---|---|---|
| 1.1 | ʻschemaType' (data field) | type of electronic message | Specify the value [antifraudRequest] - an additional request to an information exchange participant - 'the payee' in an unauthorised transaction | <pre>'header': {</pre> |
| 1.2 | 'schemaVersion' (data field) | electronic message type scheme | textarea (text field) | 'memberld': '9527dd0c-0765-4f1c-8f5f-70a02cf4046c', 'publishedAt': '2002-10-02T15:00:00.05Z' }, |
| 1.3 | 'version' (data field) | electronic message version number during information exchange | numeric value (int) | |
| 1.4 | 'memberld' (data field) | identifier of an information exchange participant assigned by the Bank of Russia | 128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by the Bank of Russia | |
| 1.5 | ʻpublishedAt' (data field) | date and time of initial provision of information | data submission format in accordance with Specification RFC 3339 [11] | |

7.2. Description of the Bank of Russia's request form. Data block [antifraudRequest]

The form of Bank of Russia's request to the information exchange participant servicing the payee shall apply:

when requesting from the money transfer operator serving the payee, including the electronic funds operator, information identifying the payee [4];

when sending a notification of the suspension of funds crediting to the payee's bank account or an increase in the balance of the payee's electronic funds [20].

| Data block (field) No. | ldentifier of data block (field) | Data block (field) content | Data field format | E-mail format |
|---------------------------------|--|---|---|---|
| 1 | ʻantifraudRequest (data block) | | If it is necessary to specify several values of data blocks (payer, payee), specify one or several objects in the data block 'antifraudRequest' | 'antifraudRequest': [{ |
| 1.1 | ʻsourceld' (data field) | identifier assigned by an information exchange participant who is the payer | 128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by the information exchange participant | 'namePayer': 'name of the organisation that is the payer', 'payerTransferId': { 'transferType': 'type of funds transfer method', |
| 1.2 | 'victim' (data field) | information on the legal status of the payer | One code is selected from the limited set of possible values: [person] – an individual; [entity] – a legal entity | 'paymentCard': { 'number': '123412341234123412', 'sum': 'the amount of a payment card money transfer transaction', 'currency': 'currency of a money transfer transaction', |
| 1.2 | 'payer' (data block) | information identifying the payer | | 'dateTimeAt': '2018-01- 13T09:14:38Z', 'rrn': 'the number generated for a |
| 1.2.1 | 'bik' (data field) | BIC of the money transfer operator serving the payer | in the AAAAAAAA format | money transfer transaction during its authorisation' }, 'settlement': { 'number': '12345123451234512345, |
| 1.2.2 | 'inn' (data field) | TIN of the payer - a legal entity, and/or an individual entrepreneur, and/or a person engaged in private business | in the XXXXXXXXXX format – for legal entities, in XXXXXXXXX or XXXXXXXXX formats – for individual entrepreneurs and (or) individuals engaged in private businesses in accordance with the procedure established by the legislation of the Russian Federation | 'sum': 'money transfer amount' - 'currency': 'currency of a money transfer transaction' - 'dateTimeAt': '2018-01- 13T09:14:38Z' }, 'phoneNumber': { 'number': (1212312345678', |

| 1.2.3 | 'payerName' (data field) | organisation name that is | textarea | 'sum': 'transaction amount', 'currency': 'transaction currency', |
|-----------|-----------------------------|---|--|--|
| | | the payer | | 'dateTimeAt': '2018-01- 13T09:14:38Z' |
| 1.2.4 | 'payerTransferId' | identification data | | }, |
| | (data subblock) | depending on the money transfer method | | ʻidNumber': { 'number': |
| | | money transfer method | | '1KoX6AA5VTdbBTkw27YEqKFaTtEQq97AAT', |
| | 'transferType' | type of money transfer | One code is selected from the | 'sum': 'transaction amount', |
| | (data field) | method | limited set of possible values: | 'currency': 'transaction currency', |
| | | | • [paymentCard] – when | 'dateTimeAt': '2018-01- 13T09:14:38Z' |
| | | | transferring funds using payment | } |
| | | | cards; [settlement] – when | }, |
| | | | transferring funds to bank accounts; | 'device': { |
| | | | • [phoneNumber] – when | 'ip': '127.0.0.1', 'imsi': 'international mobile subscriber |
| | | | transferring funds by telephone | identifier (individual subscriber number)', |
| | | | number; [idNumber] – if the balance | 'imei': 'international mobile |
| | | | of electronic funds changes | equipment identifier', 'aiic': 'Acquiring institution identification |
| | | | | code |
| | | | | (32 field ISO 8583)', |
| | | | | 'cati': 'Card acceptor terminal identification |
| 1.2.4.1 | 'paymentCard' | when transferring funds | | (41 field ISO 8583)', |
| | (data subblock) | using payment | | 'caic': 'Card acceptor identification code (42 |
| | | cards | | field ISO 8583)' |
| | | | | } |
| 1.2.4.1.1 | 'number' | number of the payer's | in the XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX | }, 'payee': { |
| | (data field) | payment card issued to | format | 'bik': '123456789', |
| | | him/her and (or) the person | | 'inn': '123456789000', 'payeeName': 'name of the organisation that is the |
| | | authorised by the payer | payment card number shall be | payee', |
| | | and the money transfer | provided without spaces (_) and | 'payeeTransferId': { |
| | | operator by the issuer | separation marks (-). | 'transferType': 'type of funds |
| 1.2.4.1.2 | 'sum' | amount of money | transaction amount - field 'F004' of | transfer method', |
| | (data field) | transferred using | ISO 8583 Financial Messages | 'number': '123412341234123412 |
| | | payment cards | Standard [7], [8], [9] | }, |
| | | | | 'settlement': { |
| | | | | 'number': '12345123451234512345' }, |
| | | | | 'phoneNumber': { |

| | | | | 'number': '1212312345678' |
|-----------|------------------------------|---|--|--|
| | | | | }, |
| 1.2.4.1.3 | 'currency' (data field) | currency of a money transfer transaction | transaction currency - field 'F049' of ISO 8583 Financial Messaging Standard [7], [8], [9] | 'idNumber': { 'number': '1KoX6AA5VTdbBTkw27YEqKFaTtEQq97AAT' |
| 1.2.4.1.4 | 'dateTimeAt' (data field) | transaction date and time | data provision format in accordance with Specification RFC 3339[11] | } } } |
| 1.2.4.1.5 | 'rrn' (data field) | number generated for a money transfer transaction during its authorisation | number generated for a money transfer transaction during its authorisation - field 'F037' < * > of ISO 8583 Financial Messaging Standard [7], [8], [9] | - }] } |
| | | | * The value of field 'F037' (Retrieval Reference Number) shall be generated by the acquiring bank host according to the following rule: | |
| | | | YJJJXXNNNNN, where: | |
| | | | Y is the last figure of a year; | |
| | | | JJJ is a Julian date; | |
| | | | XX is the identifier assigned to the acquiring bank host by the operator; | |
| | | | NNNNNN is the transaction sequence number during a day | |
| 1.2.4.2 | 'settlement' (d subblock) | when transferring funds in bank accounts by debiting money from payers' bank accounts | | |
| 1.2.4.2.1 | 'number' (data field) | the number of the payer's bank account opened with the money transfer operator serving | in the XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX | |
| | | the payer | bank account number shall be provided without spaces (_) and | |

| | | | separation marks (-). |
|-----------|----------------------------------|--|---|
| 1 2 4 2 2 | (| and a first of a first of | , |
| 1.2.4.2.2 | ʻsum' (data field) | amount of a fund transfer transaction | textarea (text field) |
| 1.2.4.2.3 | 'currency' (data field) | currency of funds transfer transaction | textarea (text field) |
| 1.2.4.2.4 | 'dateTimeAt' (data field) | transaction date and time | data provision format in accordance with Specification RFC 3339[11] |
| 1.2.4.3 | 'phoneNumber' (data subblock) | when making money transfers by telephone number | |
| 1.2.4.3.1 | 'number' (data field) | the payer's telephone number specified in a | in the KKKXXXNNNNNNN format, where: |
| | | bank account agreement and/or a agreement on | KKK – from one to three characters of the country code; |
| | | the use of electronic payment instruments | XXX – operator's code; |
| | | concluded with the payer | NNNNNNN - seven characters of the number. |
| | | | The telephone number shall be represented without a plus sign (+), spaces (_) and separation signs (-). |
| 1.2.4.3.2 | 'sum' (data field) | transaction amount | textarea (text field) |
| 1.2.4.3.3 | 'currency' (data field) | transaction currency | textarea (text field) |
| 1.2.4.3.4 | 'dateTimeAt' (data field) | transaction date and time | data provision format in accordance with Specification RFC 3339[11] |
| 1.2.4.4 | ʻidNumber' (data subblock) | if the balance of electronic funds changes | |
| 1.2.4.4.1 | 'number' (data field) | the payer's identification number, in particular, the number of the payer's electronic wallet used by him/her on the basis of a bank account agreement | textarea (text field) |

| | | and (or) an agreement | |
|-----------|-----------------|----------------------------|-------------------------------------|
| | | on the use of the | |
| | | electronic payment | |
| | | instruments concluded | |
| | | with the money transfer | |
| | | operator | |
| 1.2.4.4.2 | 'sum' | transaction amount | textarea (text field) |
| 1.2.4.4.2 | (data field) | | |
| 1.2.4.4.3 | 'currency' | transaction currency | textarea (text field) |
| | (data field) | , | · · · |
| 1.2.4.4.4 | 'dateTimeAt' | transaction date and time | data provision format in accordance |
| | (data field) | | with Specification RFC 3339 [11] |
| | | | |
| 1.2.5 | 'device' | parameters of the device | |
| | (data subblock) | used to access an | |
| | | automated system and | |
| | | software for the purpose | |
| | | of money transfer | |
| | | without | |
| | | the customer's consent | |
| | | | |
| 1.2.5.1 | 'ip' (data | network address of a | The IPv4 network address shall |
| 1.2.3.1 | field) | computer and/or a | comply with RFC 791 specification |
| | neidy | communication device | [12] |
| | | (router) (IP) | [] |
| 1.2.5.2 | 'imsi' | International Mobile | number (15-bit in decimal) AA- |
| | (data field) | Subscriber Identity (IMSI) | BBBBBB-CCCCC-EE |
| | . , | means the international | |
| | | identifier of a mobile | |
| | | subscriber (individual | |
| | | number of a subscriber | |
| | | (an individual customer) | |
| | | by which the system | |
| | | recognises a mobile | |
| | | communication user | |
| | | using GSM and UMTS | |
| | | standards | |
| 1.2.5.3 | 'imei' | International Mobile | number (15-bit in decimal) |
| 1.2.3.5 | (data field) | Equipment Identity (IMEI) | |
| | (uutu neiu) | | |

| | | international identifier of mobile equipment (mobile device of an individual customer) | AA-BBBBBBB-CCCCCC- EE |
|---------|------------------------|---|--|
| 1.2.5.4 | ʻaiic' (data field) | identifier of the participant who is an acquiring bank when transferring funds using payment cards | identifier of the participant who is an acquiring bank in the course of money transfer operations using payment cards (Acquiring institution identification code) - field 'F032' of ISO 8583 [7], [8], [9] |
| 1.2.5.5 | 'cati' (data field) | identifier of the ATM and/or the electronic terminal where funds are transferred and/or withdrawn | identifier of the ATM and/or the electronic terminal where funds are transferred and/or withdrawn (Card acceptor terminal identification) - field 'F041'* of the ISO 8583 Financial Messaging Standard [7], [8], [9] * The terminal identifier value should be aligned to the left and supplemented with spaces on the right with up to 8 characters |
| 1.2.5.6 | 'caic' (data field) | identifier of the ATM and/or the electronic terminal where funds are transferred and/or withdrawn by its geographical location | identifier of the ATM and/or the electronic terminal where funds are transferred and/or withdrawn by its geographical location (Card acceptor identification code) - field 'F042'* of ISO 8583 Financial Messaging Standard [7], [8], [9] * The value of the service point identifier shall be aligned to the left and supplemented with spaces |

| | | | on the right with up to 15 characters |
|-------|--------------------------------------|--|---|
| | | | on the right with up to 15 characters |
| 1.3 | ʻpayee' (data block) | information identifying the payee | |
| 1.3.1 | 'bik' (data field) | BIC of the money transfer operator serving the payee | in the AAAAAAAA format |
| 1.3.2 | 'inn' (data field) | TIN of the payee – a legal entity, and (or) an individual entrepreneur, and (or) a person engaged in private business | |
| 1.3.3 | 'namePayee' (data field) | name of the organisation that is the payee | textarea (text field) |
| 1.3.4 | 'payeeTransferld' (data subblock) | identification data depending on the method of a money transfer | |
| | 'transferType' (data field) | type of money transfer method | One code is selected from the limited set of possible values: • [paymentCard] – when transferring funds using payment cards; • [settlement] – when transferring funds to bank accounts; • [phoneNumber] – when transferring funds by telephone number; • [idNumber] – if the balance of electronic funds changes |

| 1.3.4.1 | 'paymentCard' (data subblock) | when transferring funds using payment cards | |
|-----------|----------------------------------|---|---|
| 1.3.4.1.1 | 'number' (data field) | number of the payment card of the payee issued to him and (or) the person authorised by the payee, the money transfer operator – the issuer | B the XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX |
| 1.3.4.2 | 'settlement' (d subblock) | when making money transfers in bank accounts by debiting funds from payers' bank accounts | |
| 1.3.4.2.1 | 'number' (data field) | the settlement account number of the payee opened with the money transfer operator serving the payee | in the XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX |
| 1.3.4.3 | 'phoneNumber' (data subblock) | when making money transfers by telephone number | |
| 1.3.4.3.1 | 'number' (data field) | the payee's phone number | in the KKKXXXNNNNNNN format, where: KKK – a country code of one to three characters; XXX – operator's code; NNNNNNN - seven characters of the number. |

| 1.3.4.4 | ʻidNumber' (data subblock) | if the balance of electronic funds changes | The telephone number shall be represented without a plus sign (+), spaces (_) and separation signs (-). |
|-----------|-------------------------------|---|---|
| 1.3.4.4.1 | 'number' (data field) | identification number of the payee, in particular, the number of the electronic wallet of the payee used by him/her on the basis of a bank account agreement and (or) an agreement on the use of electronic payment instruments concluded with the money transfer operator | |

8. The data submission form used by information exchange participants to provide a response to the Bank of Russia's request to the information exchange participant serving the payee and the timeframes for their submission to the Bank of Russia

In response to the Bank of Russia's request for verification of a particular payee specified in Chapter 7 hereof, the information shall be sent to the Bank of Russia as soon as possible, but no later than the day following the date of receipt by the information exchange participant serving the payee of the corresponding request of the Bank of Russia.

The information in response to the Bank of Russia's request regarding the suspension (impossibility to suspend) of funds crediting to the payee's bank account or the increase in the balance of the payee's electronic funds specified in Chapter 7 hereof shall be sent promptly upon receipt of the relevant request from the Bank of Russia.

8.1. Identification data of the response to the Bank of Russia's request. Data block [HEADER]

| Data block (field) No. | ldentifier of data block (field) | Data block (field) content | Data field format | E-mail format | Obligation of informing |
|---------------------------------|-------------------------------------|---|--|--|----------------------------|
| 1.1 | ʻschemaType' (data field) | type of electronic message | Specify the value of [anifraudResponse] – a response of the 'payee' of an unauthorised transaction to the Bank of Russia | { | [0] |
| 1.2 | 'schemaVersion' (data field) | electronic message type scheme | textarea (text field) | 'memberld': '9527dd0c-0765-4f1c-8f5f- 70a02cf4046c', 'sourceld': 'f34030ef-358a-445c- | [0] |
| 1.3 | 'version' (data field) | electronic message version number during information exchange | numeric value (int) | 8567-25985ce6d91c', 'publishedAt': '2002-10- 02T15:00:00.05Z' }, | [0] |
| 1.4 | ʻmemberld' (data field) | identifier of an information exchange participant assigned by the Bank of Russia | 128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] and assigned by the Bank of Russia | | [0] |
| 1.5 | ʻsourceld' (data field) | identifier assigned by an information exchange participant | 128-bit identifier (GUID) generated in accordance with Specification | | [N] |

| | | | RFC 4122 [16] assigned by an information exchange participant |
|-----|---------------|---|---|
| 1.6 | 'publishedAt' | date and time when the | data presentation format in |
| | (data field) | response to the Bank of Russia's request was | accordance with Specification RFC 3339 [11] |
| | | submitted | Specification KFC 5555 [11] |
| | | Submitted | |

8.2. Description of the response form to the Bank of Russia's request. Data block [anifraudResponse]

The data submission form for information exchange participants to provide a response to the Bank of Russia's request sent to the information exchange participant serving the payee shall be used:

when the money transfer operator serving the payee, including the electronic money operator, informs the Bank of Russia about a particular payee [4];

when sending a notification of the successful suspension of funds crediting to the payee's bank account or an increase in the balance of the payee's electronic funds [20];

when sending a notification of the impossibility to suspend funds crediting to the bank account of the payee or an increase in the balance of the payee's electronic funds [20].

| Data block (field) No. | ldentifier of data block (field) | Content of data block (field) | Data field format | E-mail format | Obligation of information provision |
|---------------------------------|-------------------------------------|---|---|---|--|
| 1 | 'antifraudRespons (data block) | | If it necessary to indicate several values of blocks of data (payer, payee, additionalStatus) one or several objects in the block of data 'antifraud' should be specified | 'anifraudResponse': [{ | [0] |
| 1.2 | ʻsourceld' (data field) | identifier assigned by an information exchange participant being the payer | 128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] and assigned by the information exchange participant | 'payeeldentifier': { | [0] |
| 1.3 | 'victim' (data field) | information on the legal status of the payer | One code shall be selected from the limited set of possible values: • [person] - an individual; • [entity] - a legal | 8FA441E44' }, 'payer': { 'bik': '123456789', 'inn': '123456789000', 'payerName': 'name of the organisation | [0] |

| | | | entity | that is the payer', | |
|-------|-----------------------------------|--|--|--|-----|
| 1.4 | ʻrecipient' (data field) | information on the legal status of the payee | One code shall be selected from the limited set of possible values: • [person] – an individual; • [entity] – a legal entity | 'payerTransferId': { | [0] |
| 1.5 | 'payeeldentifier' (data block) | identification data of a particular payee | | transfer transaction using payment cards'. 'currency': 'currency of money transfers', 'dateTimeAt': '2018- 01- 13T09:14:38Z', | [0] |
| 1.5.1 | ʻhash' (data field) | information on the result of calculating a hash function of the identification document number in order to identify the applicant(s) authorised to dispose of the funds of the payee(s) | The sequence of symbols obtained as a result of the calculation of the SHA-256 hash function from the series and number of the identification document. The series and number of the identification document are provided for calculating the hash function: without spaces (_), the number sign (N), letters (if any) in upper case (ABC). For a Russian passport, this is XXXXYYYYY, where: XXXX – four-digit passport series; YYYYYY is the six-digit passport number. Source text encoding (before hash) – Windows-1251; | <pre>'rrn': 'the number generated for a money transfer transaction during its authorisation'</pre> | [0] |

| | | | Hash text encoding – Windows-1251. | 13T09:14:38Z' } | |
|-------|-----------------------------|---|--|--|-----|
| 1.5.2 | 'hashSnils' (data field) | information on the result of the calculation of the SNILS hashing function of the payee (s) who is (are) the person(s) authorised to dispose of the funds of the payee(s) | The sequence of symbols obtained as a result of calculating the SHA-256 hash function from the payer's SNILS. SNILS is provided for calculating the hash function: without spaces (_) and separation marks (-). SNILS type: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX | }, 'device': { 'ip': '127.0.0.1', 'imsi': 'international mobile subscriber identifier (individual subscriber number)', 'imei': 'international mobile equipment identifier', 'aiic': 'Acquiring institution identification code (32 поле ISO 8583)', 'cati': 'Card acceptor terminal identifica- tion (41 поле ISO 8583)', 'caic': 'Card acceptor identification code (42 поле ISO 8583)' } }, 'payee': { | [0] |
| 1.6 | ʻpayer' (data block) | information identifying the payer | | 'bik': '123456789', 'inn': '123456789000', 'payeeName': 'name of the organisation that | [0] |
| 1.6.1 | 'bik' (data field) | BIC of the money transfer operator serving the payer | in the AAAAAAAA format | is the payee', 'payeeTransferId': { 'transferType': 'type of money transfer method', | [0] |
| 1.6.2 | 'inn' (data field) | TIN of the payer who is a legal entity, and/or an individual entrepreneur, and/or a person engaged in private business | in the XXXXXXXXX format - for legal entities, in XXXXXXXXX or XXXXXXXXX formats – for individual entrepreneurs and (or) individuals engaged in private businesses in accordance with the procedure established by the legislation of the Russian Federation. | 'paymentCard': { 'number': '123412341234123412', 'sum': 'the amount of a money transfer transaction using payment cards'. 'currency': 'the amount of a money transfer transaction using payment cards', 'status1': { 'enrollment': 'transaction suspension identifier', | [0] |
| 1.6.3 | 'payerName' (data field) | organisation name that is the payer | textarea (text field) | 'dateTimeAt': '2002- 10- 02T15:00:00.05Z' } }, | [0] |

| | | | | 'settlement': { | |
|---------------|--------------------------------------|--|--|---|-----|
| 1.6.4 | 'payerTransferId' (data subblock) | identification data depending on the money transfer method | | 'number': '12345123451234512345', 'sum': 'amount of a money transfer transaction using payment cards', | [0] |
| 1.6.4.1 | 'transferType' (data field) | type of money transfer method | One code shall be selected from the limited set of possible values: • [paymentCard] – when transferring funds using payment cards; • [settlement] – when transferring funds in bank accounts; • [phoneNumber] – when transferring funds by telephone number; • [idNumber] – when the balance of electronic money changes | 'currency': 'currency of money transfers', 'status1': { 'enrollment': 'transaction suspension identifier' 'dateTimeAt': '2002- 10- 02T15:00:00.05Z' } }, 'phoneNumber': { 'number': { 'number': '1212312345678', 'sum': 'transaction amount', 'currency': 'transaction currency', 'status1': { 'enrollment': 'transaction suspension identifier' | [0] |
| 1.6.4.2 | 'paymentCard' (data subblock) | when transferring funds using payment cards | | 10- 02T15:00:00.05Z' } | [0] |
| 1.6.4.2. 1 | 'number' (data field) | the number of a payer's payment card issued to him/her and (or) the person authorised by the payer and the money transfer operator who is the issuer | in the XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX | }, 'idNumber': { 'number': '1KoX6AA5VTdbBTkw27YEqKFaTtEQq97AAT', 'sum': 'amount of a transaction for changing the balance of funds', 'currency': 'currency of a transaction for changing the balance of funds', 'status1': { | [0] |
| 1.6.4.2. 2 | 'sum' (data field) | the amount of a money transfer transaction using payment cards | transaction amount - field 'F004' of ISO 8583 Financial Messages Standard [7], [8], [9] | status1. { 'enrollment': 'transaction suspension identifier' 02T15:00:00.05Z' } } | [0] |

| 1.6.4.2. | 'currency' | currency of a money | transaction currency – field | } | |
|---------------|------------------------------|--|--|--------|-----|
| 3 | (data field) | transfer transaction | (F049' of ISO 8583 Financial Messages Standard [7], [8], [9] | } } | [0] |
| 1.6.4.2. 4 | 'dateTimeAt' (data field) | transaction date and time | data provision format in accordance with Specification RFC 3339 [11] | | [0] |
| 1.6.4.2. | 'rrn' (data | number generated for a | the number generated for a | | |
| 5 | field) | money transfer transaction during its authorisation | money transfer transaction during its authorisation - field 'F037'* of ISO 8583 Financial Messages Standard [7], [8], [9] * The value of field 'F037' (Retrieval Reference Number) | | |
| | | | shall be generated by the acquiring bank host according to the following rule: | | [0] |
| | | | YJJJXXNNNNNN, where: | | 1 |
| | | | Y is the last figure of a year; | | |
| | | | JJJ is a Julian date; | | |
| | | | XX is the identifier assigned to the acquiring bank host by the operator; | | |
| | | | NNNNNN is the transaction sequence number during a day | | |
| 1.6.4.3 | 'settlement' | when transferring funds in | | | |
| | (data subblock) | bank accounts by debiting money from payers' bank accounts | | | [0] |
| 1.6.4.3. 1 | 'number' (data field) | bank account number of the payer opened with | in the | | [O] |

| | | the money transfer operator serving the payer | XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX |
|--------------------|--|---|---|
| | | | bank account number shall be provided without spaces (_) and separation marks (-). |
| 1.6.4.3. 2 | 'sum' (data field) | amount of a fund transfer transaction | textarea (text field) |
| 1.6.4.3. 3 | 'currency' (data field) | | textarea (text field) |
| 1.6.4.3. 4 | 'dateTimeAt' (data field) | transaction date and time | data provision format in accordance with Specification RFC 3339 [11] |
| 1.6.4.4 | 'phoneNumber' (data subblock) | when making money transfers by telephone number | |
| 1.6.4.4. 1 | 'number' (data field) | the payer's telephone number specified in a bank account agreement and/or a agreement on the use of electronic payment instruments concluded with the payer | in the KKKXXXNNNNNNN format, where: KKK – from one to three characters of the country code; XXX – operator's code; NNNNNNN - seven characters of the number. The telephone number shall be represented without a plus sign (+), spaces (_) and |
| 1.6.4.4. | 'sum' | transaction amount | separation signs (-). textarea (text field) |
| 2 1.6.4.4. 3 | (data field) 'currency' (data field) | transaction currency | textarea (text field) |
| 1.6.4.4. 4 | 'dateTimeAt' (data field) | transaction date and time | data provision format in accordance with Specification RFC 3339 [11] |
| 1.6.4.5 | ʻidNumber' (data subblock) | if the balance of electronic funds changes | |

| 1.6.4.5. 1 | 'number' (data field) | the payer's identification number, in particular, the number of the payer's electronic wallet used by him/her on the basis of a bank account agreement and (or) an agreement on the use of electronic payment instruments concluded with the money transfer operator | textarea (text field) |
|---------------|------------------------------|--|---|
| 1.6.4.5. 2 | 'sum' (data field) | transaction amount | textarea (text field) |
| 1.6.4.5. 3 | 'currency' (data field) | transaction currency | textarea (text field) |
| 1.6.4.5. 4 | 'dateTimeAt' (data field) | transaction date and time | data provision format in accordance with Specification RFC 3339 [11] |
| 1.6.5 | 'device' (data subblock) | parameters of the device used to access the automated system and software for the purpose of transferring funds without the customer's consent | |
| 1.6.5.1 | 'ip' (data field) | | The IPv4 network address shall comply with Specification RFC 791 [12] |
| 1.6.5.2 | 'imsi' (data field) | International Mobile Subscriber Identity (IMSI) means the international identifier of a mobile subscriber (individual number of a subscriber (individual customer) by which the system recognises a mobile communication user using GSM and UMTS standards | number (15-bit in decimal) AA-BBBBBB-CCCCCC-EE |

| 1.6.5.3 | 'imei' (data field) | International Mobile Equipment Identity (IMEI) – international identifier | number (15-bit in decimal) AA-BBBBBB-CCCCCC-EE |
|---------|------------------------|---|---|
| | | of mobile equipment (mobile device of an individual customer) | |
| 1.6.5.4 | ʻaiic' (data field) | identifier of the participant who is an | identifier of the participant who is an acquiring bank |
| | | acquiring bank when it transfers funds using payment cards | during money transfer transactions using payment cards (Acquiring institution |
| | | payment calus | identification code) - field 'F032' of ISO 8583 [7], [8], [9] |
| | | | |
| 1.6.5.5 | 'cati' | identifier of the ATM | identifier of the ATM and/or |
| | (data field) | and/or the electronic terminal where funds are | the electronic terminal where funds are transferred |
| | | transferred and/or withdrawn | and/or withdrawn (Card acceptor terminal identification) – field |
| | | | 'F041'* of ISO 8583 Financial Messages Standard [7], |
| | | | [8], [9] |
| | | | * The value of the terminal identifier shall be aligned to |
| | | | the left and supplemented with spaces on the right |
| | | | with up to 8 characters |
| 1.6.5.6 | 'caic' | identifier of the ATM | identifier of the ATM and/or |

| | (data field) | and/or the electronic terminal funds are transferred and/or withdrawn by its geographical location | the electronic terminal where funds are transferred and/or withdrawn by its geographical location (Card acceptor identification code) - field 'F042'* of ISO 8583 Financial Messaging Standard [7], [8], [9] * The value of the service point identifier shall be aligned to the left and supplemented with spaces or the right with up to 15 characters |
|-------|--------------------------------------|--|---|
| 1.7 | 'payee' (data block) | information identifying | |
| 174 | | the payee | |
| 1.7.1 | 'bik' (data field) | BIC of the money transfer operator serving the payee | in the AAAAAAAA format |
| 1.7.2 | 'inn' (data field) | TIN of the payee – a legal entity, and (or) an individual entrepreneur, and (or) a person engaged in private business | in the XXXXXXXXX format - for legal entities, in XXXXXXXXX or XXXXXXXX formats – for individual entrepreneurs and (or) individuals engaged in private businesses in accordance with the procedure established by the legislation of the Russian Federation |
| 1.7.3 | 'payeeName' (data field) | name of the organisation that is the payee | textarea (text field) |
| 1.7.4 | 'payeeTransferId' (data subblock) | identification data depending on the | |

| 4744 | | money transfer method | |
|---------------|----------------------------------|---|--|
| 1.7.4.1 | 'transferType' (data field) | type of money transfer method | One code shall be selected from the limited set of possible values: • [paymentCard] – when transferring funds using payment cards; • [settlement] – when transferring funds in bank accounts; • [phoneNumber] – when transferring funds by telephone number; • [idNumber] – when the balance of electronic money changes |
| 1.7.4.2 | 'paymentCard' (data subblock) | when transferring funds using payment cards | |
| 1.7.4.2. 1 | 'number' (data field) | number of the payment card of the payee issued to him/her and (or) the person authorised by the payee, the money transfer operator – the issuer | in the XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX |
| 1.7.4.2. 2 | 'sum' (data field) | the amount of a money transfer transaction using payment cards | transaction amount - field 'F004' of ISO 8583 Financial Messages Standard [7], [8], [9] |
| 1.7.4.2. 3 | 'currency' (data field) | currency of a money transfer transaction | transaction currency – field 'F049' of ISO 8583 Financial Messages Standard [7], [8], [9] |

| 1.7.4.2. | 'status1' | transaction suspension | |
|----------------------|---------------------------------|---|---|
| 4 | (data subblock) | status | |
| 4 1.7.4.2. 4.1 | | status transaction suspension identifier | One code shall be selected from the limited set of possible values: • [successful] – successful suspension of funds crediting to the payee's bank account or suspension of increasing the balance of the payee's electronic funds; • [unsuccessful] – it is impossible to suspend funds crediting to the payee's bank account or to suspend increasing the balance of the payee's electronic funds |
| 1.7.4.2. 4.2 | 'dateTimeAt' (data field) | date and time of suspending (failure to suspend) funds crediting to the payee's bank account or suspending (failure to suspend) the increase in the balance of the payee's electronic funds | data provision format in accordance with Specification RFC 3339 [11] |
| 1.7.4.3 | 'settlement' (data subblock) | when transferring funds in bank accounts by debiting money from payers' bank accounts | |

| 1.7.4.3. 1 | 'number' (data field) | the settlement account number of the payee opened with the money transfer operator serving the payee | in the XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX |
|-----------------|------------------------------|---|---|
| 1.7.4.3. | 'sum' | amount of a transaction | textarea (text field) |
| 2 | (data field) | to transfer funds | |
| 1.7.4.3. | 'currency' | currency of a fund | textarea (text field) |
| 3 | (data field) | transfer transaction | |
| 1.7.4.3. | ʻstatus1' | transaction suspension | |
| 4 | (data subblock) | status | |
| 1.7.4.3. 4.1 | ʻenrollment' (data field) | transaction suspension identifier | One code shall be selected from the limited set of possible values: • [successful] – successful suspension of funds crediting to the payee's bank account or suspension of increasing the balance of the payee's electronic funds; • [unsuccessful] – it is impossible to suspend funds crediting to the payee's bank account or to suspend increasing the balance of the payee's electronic funds |
| 1.7.4.3. 4.2 | 'dateTimeAt' (data field) | date and time of suspending (failure to suspend) funds crediting to the payee's bank account or suspending (failure to suspend) the increase in the balance of the payee's electronic funds | data provision format in accordance with Specification RFC 3339 [11] |

| | | - | |
|-----------------|------------------------------|--|---|
| | | | |
| | | | |
| 1.7.4.4 | 'phoneNumber' | when making money transfers by telephone | |
| | (data subblock) | number | |
| | | | • |
| 1.7.4.4. 1 | 'number' (data field) | the payee's phone number | in the KKKXXXNNNNNNN |
| | | | format, where: |
| | | | KKK – from one to three characters of the country |
| | | | code; |
| | | | XXX – operator's code; |
| | | | NNNNNN - seven characters |
| | | | of the number. |
| | | | The telephone number shall |
| | | | be represented without a |
| | | | plus sign (+), spaces (_) and separation signs (-). |
| 1.7.4.4. | 'sum' | 'sum' | transaction amount |
| 2 1.7.4.4. | (data field) | (data field) | |
| 1.7.4.4. 3 | 'currency' (data field) | 'currency' (data field) | transaction currency |
| 1.7.4.4. 4 | ʻstatus1' (data subblock) | transaction suspension status | |
| | | status | |
| 1.7.4.4. 4.1 | ʻenrollment' (data field) | transaction suspension | One code shall be selected from the limited |
| 7.1 | (uata ficia) | identifier | set of possible values: |
| | | | • [successful] – successful |
| | | | suspension of funds crediting to the payee's bank account |
| | | | or suspension of increasing |
| | | | the balance of the payee's electronic funds; |
| | | | • [unsuccessful] – it is |
| | | | impossible to suspend |

STO BR BFBO-1.5-

| | | | the crediting of funds to the payee's bank account or to suspend the increase in the balance of the recipient of electronic funds |
|-----------------|-------------------------------|---|---|
| 1.7.4.4. 4.2 | 'dateTimeAt' (data field) | date and time of suspending (failure to suspend) funds crediting to the payee's bank account or suspending (failure to suspend) the increase in the balance of the payee's electronic funds | data provision format in accordance with Specification RFC 3339 [11] |
| 1.7.4.5 | ʻidNumber' (data subblock) | if the balance of electronic funds changes | |
| 1.7.4.5. 1 | 'number' (data field) | identification number of the payee, in particular, the number of the electronic wallet of the payee used by him/her on the basis of a bank account agreement and (or) an agreement on the use of the electronic payment instruments concluded with the money transfer operator | textarea (text field) |
| 1.7.4.5. 2 | ʻsum' (data field) | transaction amount | textarea (text field) |
| 1.7.4.5. 3 | 'currency' (data field) | transaction currency | textarea (text field) |
| 1.7.4.5. 4 | ʻstatus1' (data subblock) | transaction suspension status | |

| 1.7.4.5. | . 'enrollment' | transaction | One code shall be |
|-----------------|--------------------------------|---|---|
| 4.1 | (data field) | suspension identifier | selected from the limited set of possible values: |
| | | | [successful] – successful suspension of funds crediting to the payee's bank account or suspension of increasing the balance of the payee's electronic funds; [unsuccessful] – it is impossible to suspend funds crediting to the payee's bank account or to suspend increasing the balance of the payee's electronic funds |
| 1.7.4.5. 4.2 | . 'dateTimeAt' (data field) | date and time of suspending (failure to suspend) funds crediting to the payee's bank account or suspending (failure to suspend) the increase in the balance of the payee's electronic funds | data provision format in accordance with Specification RFC 3339 [11] |

The form of the Bank of Russia's information message shall apply to the information exchange participant serving the payer as follows:

when sending a notification on the successful suspension of funds crediting to the payee's bank account or suspension of increasing the balance of the payee's electronic funds [20];

when sending a notification of the impossibility to suspend funds crediting to the bank account of the payee or increasing the balance of the payee's electronic funds [20];

9.1. Identification data of the Bank of Russia's information message to the information exchange participant serving the payer. Data block **[HEADER]**

| Data block (field) No. | ldentifier of data block (field) | Data block (field) content | Data field format | E-mail format |
|---------------------------------|-------------------------------------|---|---|--|
| 1.1 | 'schemaType' (data field) | type of electronic message | Specify value [antifraudReturn] – additional request to the information exchange participant who is the 'payee' of an unauthorised transaction | { |
| 1.2 | 'schemaVersion' (data field) | electronic message type scheme version | textarea (text field) | 'publishedAt': '2002-10-02T15:00:00.05Z' }, |
| 1.3 | 'version' (data field) | electronic message version number during information exchange | numeric value (int) | |
| 1.4 | 'memberld' (data field) | information exchange | 128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by the Bank of Russia | |
| 1.5 | ʻpublishedAt' (data field) | date and time of initial provision of information | data submission format in accordance with Specification RFC 3339 [11] | |

9.2. Description of the form of the Bank of Russia's information message to the information exchange participant serving the payer. Data block **[anifraudReturn]**

| Data block (field) No. | ldentifier of data block (field) | Content of data block (field) | Data field format | E-mail format |
|---------------------------------|-------------------------------------|--|---|---|
| 1 | ʻanifraudReturn' (data block) | | If it is necessary to specify several values of data blocks (payer, payee), specify one or several objects in the data block 'antifraudReturn' | 'anifraudReturn': [{ |
| 1.1 | ʻsourceld' (data field) | | 128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by an information exchange participant | <pre>'inn': '123456789000',</pre> |
| 1.2 | 'victim' (data field) | information on the legal status of the payer | One code should be selected from the limited set of possible values: [person] – an individual; [entity] – a legal entity | 'number': '123412341234123412', 'sum': 'amount of a money transfer transaction using payment cards', 'currency': 'currency of a transaction to transfer funds', |
| 1.3. | 'recipient' (data field) | information on the legal status of the payee | One code should be selected from the limited set of possible values: • [person] – an individual; • [entity] – a legal entity | |
| 1.4 | ʻpayer' (data block) | information identifying the payer | | to transfer funds' |
| 1.4.1 | 'bik' (data field) | BIC of the money transfer operator serving the payer | in the AAAAAAAA format | to transfer funds' to transfer funds', 'dateTimeAt': '2018-01-13T09:14:38Z' }, 'phoneNumber': { |
| 1.4.2 | 'inn' (data field) | TIN of the payer – a legal | in the XXXXXXXXXX format – for legal entities, in XXXXXXXXX or | pronerationer . (|

| | | entity, and/or an individual entrepreneur, and/or a person engaged in private business | XXXXXXXXXXX formats – for individual entrepreneurs and (or) individuals engaged in private businesses in accordance with the procedure established by the legislation of the Russian Federation. | <pre>'number': '1212312345678',</pre> |
|---------------|--------------------------------------|---|--|---|
| 1.4.3 | 'payerName' (data field) | organisation name that is the payer | textarea (text field) | '1KoX6AA5VTdbBTkw27YEqKFaTtEQq97AAT', 'sum': 'transaction amount', 'currency': 'transaction currency', |
| 1.4.4 | 'payerTransferld' (data subblock) | identification data depending on the method of a money transfer | | 'dateTimeAt': '2018-01-13T09:14:38Z' }, 'device': { 'ip': '127.0.0.1', 'imsi': 'international mobile subscriber identifier |
| 1.4.4.1 | 'transferType' (data field) | type of a money transfer method | One code should be selected from the limited set of possible values: | (individual subscriber number)', 'imei': 'international mobile equipment identifier', |
| | | | [paymentCard] – when transferring funds using payment cards; [settlement] – when transferring funds in bank accounts; [phoneNumber] – when transferring funds by a subscriber's telephone number; [idNumber] – when the balance of electronic funds changes | 'aiic': 'Acquiring institution identification code (32 поле ISO 8583)', 'cati': 'Card acceptor terminal identification (41 поле ISO 8583)', 'caic': 'Card acceptor identification code (42 поле ISO 8583)' } }, 'payee': { |
| 1.4.4.2 | 'paymentCard' (data subblock) | when transferring funds using payment cards | | 'bik': '123456789 'inn': '123456789000', 'payeeName': 'name of the organisation that is the payee', 'payeeTransferId': { 'transferType': 'type of money transfer method', |
| 1.4.4.2. 1 | 'number' (data field) | the number of the payer's payment card issued to him and (or) a person | в the XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX | 'paymentCard': { 'number': '123412341234123412', 'sum': 'amount of a money transfer transaction using payment cards', 'currency': 'currency of a transaction to transfer funds using payment cards', |

| | | authorised by the payer and the money transfer operator by the | and separation marks (-). | 'status1': { |
|---------------|---------------------------------|--|--|--|
| | | issuer | | 'dateTimeAt':'2002-10- 02T15:00:00.05Z' |
| 1.4.4.2. 2 | 'sum' (data field) | amount of the money transfer transaction using payment cards | transaction amount - field 'F004' of ISO 8583 Financial Messages Standard [7], [8], [9] | } }, 'settlement': { 'number': '12345123451234512345', 'sum': 'amount of a fund transfer transaction', |
| 1.4.4.2. 3 | 'currency' (data field) | currency of the money transfer transaction | transaction currency - field 'F049' of ISO 8583 Financial Messaging Standard [7], [8], [9] | 'currency': 'currency of a transaction to transfer funds', 'status1': { 'enrollment': 'transaction |
| 1.4.4.2. 4 | 'dateTimeAt' (data field) | transaction date and time | data provision format in accordance with Specification RFC 3339[11] | suspension identifier', - 'dateTimeAt':'2002-10- |
| 1.4.4.2. 5 | 'rrn' (data field) | generated for a money transfer transaction during its authorisation | number generated for a money transfer transaction during its authorisation – field 'F037'* of ISO 8583 Financial Messaging Standard [7], [8], [9] * The value of field 'F037' (Retrieval Reference Number) shall be generated by the acquiring bank host according to the following rule: YJJJXXNNNNN, where: Y is the last figure of a year; JJJ is a Julian date; XX is the identifier assigned to the acquiring bank host by the operator; NNNNN is the transaction sequence number during a day | <pre>' 'dateTimeAt':'2002-10- 02T15:00:00.05Z' } }, 'idNumber': {</pre> |
| 1.4.4.3 | 'settlement' (data subblock) | when transferring funds in bank accounts | | 'currency': 'currency of the transaction for changing the balance of funds', 'status1': { 'enrollment': 'transaction suspension identifier', |
| | | by debiting funds from payers' bank accounts | | 02T1 | 15:00:00 | | } | } | } | 'dateTimeAt': 10- | '2002· |
|---------------|----------------------------------|---|--|---------------|----------|---|---|---|---|----------------------|--------|
| 1.4.4.3. 1 | 'number' (data field) | the number of the payer's bank account opened with the money transfer operator serving the payer | In the XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX | C } | }] | } | | | | | |
| 1.4.4.3. 2 | 'sum' (data field) | money transfer amount | textarea (text field) | | | | | | | | |
| 1.4.4.3. 3 | 'currency' (data field) | money transfer currency | textarea (text field) | | | | | | | | |
| 1.4.4.3. 4 | | transaction date and time | data provision format in accordance with Specification RFC 3339[11] | | | | | | | | |
| 1.4.4.4 | 'phoneNumber' (data subblock) | when transferring funds by a subscriber's telephone number | | | | | | | | | |
| 1.4.4.4. 1 | 'number' (data field) | the payer's telephone number specified in the bank account agreement and/or the agreement on the use of the electronic payment instruments concluded with | KKK – a country code of one to three characters; XXX – operator's code; NNNNNNN - seven characters of the number. The telephone number shall be | | | | | | | | |
| | | concluded with the payer | The telephone number shall be represented without a plus sign (+), spaces (_) and separation signs (-). | | | | | | | | |

| 1.4.4.4. 2 | 'sum' (data field) | transaction amount | textarea (text field) |
|---------------|------------------------------|--|--|
| 1.4.4.4. | 'currency' | transaction | textarea (text field) |
| 3 | (data field) | currency | |
| 1.4.4.4. 4 | 'dateTimeAt' (data field) | transaction date and time | data provision format in accordance with Specification RFC 3339 [11] |
| 4 | (data neid) | and time | with specification RFC 3339 [11] |
| 1.4.4.5 | 'idNumber' | if the balance of | |
| | (data subblock) | electronic funds | |
| | | changes | |
| 1.4.4.5. | 'number' | the payer's | textarea (text field) |
| 1 | (data field) | identification | |
| | | number, in particular, the | |
| | | number of the | |
| | | payer's electronic | |
| | | wallet used by him on the basis | |
| | | of a bank account | |
| | | agreement and | |
| | | (or) an agreement on the use of the | |
| | | electronic | |
| | | payment | |
| | | instruments | |
| | | concluded with the money | |
| | | transfer operator | |
| 1.4.4.5. | 'sum' | transaction | textarea (text field) |
| 2 1.4.4.5. | (data field) 'currency' | amount transaction | textarea (text field) |
| 3 | (data field) | currency | |
| 1.4.4.5. | 'dateTimeAt' | transaction date | data provision format in accordance |
| 4 | (data field) | and time | with Specification RFC 3339 [11] |
| 1.4.5 | 'device' | parameters of | |
| | (data subblock) | the device used to access | |
| | | to access | |

| | | the automated system and software for the purpose of money transfer without the customer's consent | |
|---------|------------------------|---|---|
| 1.4.5.1 | 'ip' (data field) | network address of a computer and/or a communication device (router) (IP) | The IPv4 network address shall comply with Specification RFC 791 [12] |
| 1.4.5.2 | 'imsi' (data field) | International Mobile Subscriber Identity (IMSI) means the international identifier of a mobile subscriber (individual number of a subscriber (an individual customer) with which the system recognises a mobile communication user using GSM and UMTS standards | number (15-bit in decimal) AA- BBBBBB-CCCCCC-EE |
| 1.4.5.3 | 'imei' (data field) | International Mobile Equipment Identity (IMEI) - international identifier of mobile equipment (mobile device of an individual customer) | number (15-bit in decimal) AA- BBBBBB-CCCCCC-EE |

| | | - | |
|---------|-------------------------|---|--|
| 1.4.5.4 | ʻaiic' (data field) | | identifier of the participant who is an acquiring bank in the course of money transfer transactions using payment cards (Acquiring institution identification code) - field 'F032' of ISO 8583 [7], [8], [9] |
| 1.4.5.5 | ʻcati' (data field) | | identifier of the ATM and/or electronic terminal where the funds are transferred and/or withdrawn (Card acceptor terminal identification) - field 'F041'* of the ISO 8583 Financial Messaging Standard [7], [8], [9] * The terminal identifier value shall be aligned to the left and supplemented with spaces on the right with up to 8 characters |
| 1.4.5.6 | 'caic' (data field) | identifier of the ATM and/or electronic terminal where the funds are transferred and/or withdrawn by its geographical location | identifier of the ATM and/or electronic terminal where the funds are transferred and/or withdrawn by its geographical location (Card acceptor identification code) field 'F042'* of ISO 8583 Financial Messaging Standard [7], [8], [9] * The service point identifier value shall be aligned to the left and supplemented with spaces on the right with up to 15 characters |
| 1.5 | ʻpayee' (data block) | information identifying the payee | |

| | | - | |
|---------|--------------------------------------|--|--|
| 1.5.1 | 'bik' (data field) | BIC of the money transfer operator serving the payee | in the AAAAAAAA format |
| 1.5.2 | 'inn' (data field) | TIN of the payee that is a legal entity, and (or) an individual entrepreneur, and (or) a person engaged in private business | in the XXXXXXXXX format - for legal entities, in XXXXXXXXX or XXXXXXXXX formats - for individual entrepreneurs and (or) individuals engaged in private businesses in accordance with the procedure established by the legislation of the Russian Federation |
| 1.5.3 | 'payeeName' (data field) | the name of the organisation that is the payee | textarea (text field) |
| 1.5.4 | 'payeeTransferld' (data subblock) | identification data depending on the money transfer method | |
| 1.5.4.1 | 'transferType' (data field) | type of a money transfer method | One code should be selected from the limited set of possible values: [paymentCard] – when transferring funds using payment cards; [settlement] – when transferring funds in bank accounts; [phoneNumber] – when transferring funds by a subscriber's telephone number; [idNumber] – if the balance of electronic funds changes |

| 1.5.4.2 | 'paymentCard' | when transferring | |
|---------------|--------------------------|-------------------------------------|---|
| 1.3.4.2 | (data subblock) | funds using | |
| | | payment cards | |
| | | | |
| | | | |
| 1.5.4.2. 1 | 'number' (data field) | number of the payment card of | in the XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX |
| 1 | (uata nelu) | the payee issued | format |
| | | to him/her and | payment card number shall be |
| | | (or) the person authorised by the | provided without spaces () and |
| | | payee, by the | separation marks (-). |
| | | money transfer | |
| | | operator – the issuer | |
| 1.5.4.2. | 'sum' | amount of the | transaction amount - field 'F004' of |
| 2 | (data field) | money transfer transaction using | ISO 8583 Financial Messages Standard [7], [8], [9] |
| | | payment cards | |
| | | | |
| 1.5.4.2. | 'currency' | currency of the | transaction currency – field 'F049' of |
| 3 | (data field) | money transfer | ISO 8583 Financial Messages Standard |
| | | transaction | [7], [8], [9] |
| 1.5.4.2. | 'status1' | transaction | |
| 4 | (data subblock) | suspension status | |
| 1.5.4.2. | 'enrollment' | transaction | One code should be selected from the |
| 4.1 | (data field) | suspension identifier | limited set of possible values: |
| | | luentiner | • [successful] – successful suspension of funds crediting to the |
| | | | payee's bank account or suspension |
| | | | of increasing the balance of the |
| | | | payee's electronic funds; [unsuccessful] – it is impossible to |
| | | | suspend funds crediting to the payee's |
| | | | bank account or to suspend |
| | | | |

| | | 1 | 1 |
|----------|-----------------|------------------------------------|--|
| | | | increasing the balance of the payee's |
| | | | electronic funds |
| | | | |
| 1.5.4.2. | 'dateTimeAt' | date and time of | data provision format in accordance |
| 4.2 | (data field) | suspending | with Specification RFC 3339[11] |
| | | (failure to suspend) funds | |
| | | crediting to the | |
| | | payee's bank | |
| | | account or | |
| | | suspending | |
| | | (failure to | |
| | | suspend) an | |
| | | increase in the | |
| | | balance of the | |
| | | payee's electronic | |
| | | funds | |
| | | | |
| | | | |
| 1 5 4 2 | 'settlement' | | |
| 1.5.4.3 | (data subblock) | when transferring funds in bank | |
| | (uata subbiock) | accounts by | |
| | | debiting them | |
| | | from payers' bank | |
| | | accounts | |
| | | | |
| | | | |
| | | | |
| 1.5.4.3. | 'number' | the settlement | In the XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX |
| 1 | (data field) | account number | format |
| | | of the payee | |
| | | opened with the | bank account number shall be |
| | | money transfer | provided without spaces (_) and |
| | | operator serving | separation marks (-). |
| | | the payee | separation marks (-). |
| | | | |
| 1.5.4.3. | 'sum' | money transfer | textarea (text field) |
| 2 | (data field) | amount | |
| _ | (/ | | |

| 1.5.4.3. | 'currency' | monoutransfor | textarea (text field) |
|-----------------|----------------------------------|---|--|
| 1.5.4.3. 3 | (data field) | money transfer currency | |
| 5 | (uata neiu) | currency | |
| 1.5.4.3. | 'status1' | transaction | |
| 4 | (data subblock) | suspension | |
| | (, | status | |
| 1.5.4.3. 4.1 | ʻenrollment' (data field) | transaction suspension identifier | One code should be selected from the limited set of possible values: [successful] – successful suspension of funds crediting to the payee's bank account or suspension of increasing the balance of the payee's electronic funds; [unsuccessful] – it is impossible to suspend funds crediting to the payee's bank account or to suspend |
| 1.5.4.3. | 'dateTimeAt' | date and time of | increasing the balance of the payee's electronic funds |
| 4.2 | (data field) | suspending (failure to suspend) funds crediting to the payee's bank account or suspending (failure to suspend) an increase in the balance of the payee's electronic funds | with Specification RFC 3339[11] |
| 1.5.4.4 | 'phoneNumber' (data subblock) | when ransferring funds by a | |

| | | subscriber's | |
|-----------------|----------------------------|-------------------------------|---|
| | | telephone | |
| 1.5.4.4. | 'number' | number payee's phone | in the KKKXXXNNNNNNN format, |
| 1.5.4.4. | (data field) | number | where: |
| | | | KKK – a country code of one to three |
| | | | characters; |
| | | | XXX – operator's code; |
| | | | NNNNNNN - seven characters of the number. |
| | | | The telephone number shall be |
| | | | represented without a plus sign (+), |
| | | | spaces (_) and separation signs (-). |
| 1.5.4.4. 2 | ʻsum' (data field) | 'sum' (data field) | transaction amount |
| 1.5.4.4. 3 | 'currency' (data field) | 'currency' (data field) | transaction currency |
| 1.5.4.4. | 'status1' | transaction | |
| 4 | (data subblock) | suspension status | |
| 1.5.4.4. 4.1 | 'enrollment' | transaction | One code should be selected from the |
| 4.1 | (data field) | suspension identifier | limited set of possible values: |
| | | luciturier | • [successful] – successful suspension of funds crediting to the |
| | | | payee's bank account or suspension |
| | | | of increasing the balance of the |
| | | | payee's electronic funds; |
| | | | • [unsuccessful] – it is impossible |
| | | | to suspend funds crediting to the payee's bank account or to suspend |
| | | | increasing the balance of the payee's |
| | | | electronic funds |
| | | | |
| 1.5.4.4. | 'dateTimeAt' | date and time of | data provision format in accordance |
| 4.2 | (data field) | suspending | with Specification RFC 3339 [11] |
| | | (failure to suspend) funds | |
| | | crediting to the | |
| | | payee's | |

| | | bank account or suspending (failure to suspend) increasing in the | |
|---------------|-------------------------------|--|-----------------------|
| | | balance of the payee's electronic funds | |
| 1.5.4.5 | ʻidNumber' (data subblock) | if the balance of electronic funds changes | |
| 1.5.4.5. 1 | 'number' (data field) | identification number of the payee, in particular, the number of the electronic wallet of the payee used by him/her on the basis of a bank account agreement and (or) an agreement on the use of electronic payment instruments concluded with the money transfer operator | |
| 1.5.4.5. 2 | ʻsum' (data field) | transaction amount | textarea (text field) |
| 1.5.4.5. 3 | 'currency' (data field) | transaction currency | textarea (text field) |
| 1.5.4.5. 4 | ʻstatus1' (data subblock) | transaction suspension | |

| 1.5.4.5. | 'enrollment' | transaction | One code should be selected from the |
|----------|--------------|-----------------------------------|---------------------------------------|
| 4.1 | (data field) | suspension | limited set of possible values: |
| | | identifier | • [successful] – successful |
| | | | suspension of funds crediting to the |
| | | | payee's bank account or suspension |
| | | | of increasing the balance of the |
| | | | payee's electronic funds; |
| | | | • [unsuccessful] – it is impossible |
| | | | to suspend funds crediting to the |
| | | | payee's bank account or to suspend |
| | | | increasing the balance of the payee's |
| | | | electronic funds |
| | | | |
| | | | |
| 1.5.4.5. | 'dateTimeAt' | date and time of | data provision format in accordance |
| 4.2 | (data field) | suspending | with Specification RFC 3339[11] |
| | | (failure to | |
| | | suspend) funds | |
| | | crediting to the | |
| | | payee's bank | |
| | | account or | |
| | | suspending | |
| | | (failure to | |
| | | suspend) an | |
| | | increase in the balance of the | |
| | | payee's electronic | |
| | | funds | |
| | | Tunus | |
| | | | |
| | | | |
| | | | |

10. The form for submitting a request to the Bank of Russia from information request participants who are not structural units of the Bank of Russia using the speedy and non-speedy money transfer services, about imposing (or lifting) restrictions on their bank (correspondent) accounts (sub-accounts) in the form of a ban to debit funds upon detecting incidents related to violations of data protection requirements during money transfers at the information infrastructure facilities of information exchange participants

Mandatory information provision conditions:

[O] – data block (field) information shall be provided as required;

[N] – data block (field) information shall be provided if it is technically feasible.

Time-response characteristics of information provision:

Information on imposing restrictions on bank (correspondent) accounts (sub-accounts) in the form of a ban on debiting funds upon detecting incidents related to a violation of information protection requirements during money transfers at information infrastructure facilities of information exchange participants shall be sent immediately upon detection of the relevant incident.

The data submission form used by information exchange participants for sending a request to the Bank of Russia to impose restrictions on their bank (correspondent) accounts (sub-accounts) in the form of a ban on debiting funds in the event of detection of incidents related to a violation of data protection requirements shall be applied as follows:

when the Bank of Russia is informed by information exchange participants who are not Bank of Russia structural units using the express money transfer service and the non-rapid money transfer service about imposing restrictions on their banks (correspondent) accounts (subaccounts) in the form of a ban on debiting funds upon detecting incidents related to violations of data protection requirements during money transfers at the information infrastructure facilities of information exchange participants [21];

when the Bank of Russia is informed by information exchange participants who are not Bank of Russia structural units using the speedy money transfer service and the non-speedy money transfer service about lifting restrictions in the form of a ban on debiting funds on their banks (correspondent) accounts (sub-accounts) upon detecting incidents related to violations of information protection requirements during money transfers at the information infrastructure facilities of information exchange participants [21]. **10.1.** Identification data of a request of information exchange participants to the Bank of Russia to impose (or lift) the restriction on their bank (correspondent) accounts (sub-accounts) in the form of a ban on debiting funds upon detecting incidents related to a violation of data protection requirements. Data block **[HEADER]**

| Data block (field) No. | ldentifier of data block (field) | Data block (field) content | Data field format | E-mail format | Obligation of informing |
|---------------------------------|-------------------------------------|---|---|------------------------|----------------------------|
| 1.1 | ʻschemaType' (data field) | type of electronic message | Specify the value of [lockRequest] – a request of information exchange participants to impose or lift the restriction on debiting funds on their bank (correspondent) accounts (sub-accounts) | { | [0] |
| 1.2 | 'schemaVersion' (data field) | electronic message type scheme | textarea (text field) | 02T15:00:00.05Z' }, | [0] |
| 1.3 | 'version' (data field) | electronic message version number during information exchange | numeric value (int) | | [0] |
| 1.4 | ʻmemberld' (data field) | identifier of an information exchange participant assigned by the Bank of Russia | 128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] and assigned by the Bank of Russia | | [0] |
| 1.5 | ʻsourceld' (data field) | identifier assigned by an information exchange participant | 128-bit identifier (GUID) generated in accordance with RFC specification 4122 [16] assigned by an information exchange participant | | [N] |
| 1.6 | ʻpublishedAt' (data field) | date and time when the request was submitted to the Bank of Russia | data presentation format in accordance with Specification RFC 3339 [11] | | [0] |

10.2. Description of a request of information exchange participants to the Bank of Russia to impose (or lift) the restriction on their bank (correspondent) accounts (sub-accounts) in the form of a ban on debiting funds upon detecting incidents related to a violation of data protection requirements. Data block **[lockRequest]**

| Data block (field) No. | ldentifier of data block (field) | Data block (field) content | Data field format | E-mail format | Obligation of informing |
|---------------------------------|-------------------------------------|---|---|--|----------------------------|
| 2.1 | ʻsourceld' (data field) | identifier assigned by an information exchange participant | 128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by an information exchange participant | 'lockRequest': [{ | [0] |
| 2.2 | ʻorgBik' (data field) | BIC of an information exchange participant | In the AAAAAAAAA format | debiting', 'dateAt': '20180101', | [0] |
| 2.3 | ʻregNumber' (data field) | registration number from the register of state registration of credit institutions | textarea (text field) | 'text': 'additional description','persons': { | [0] |
| 2.4. | ʻuniqldentifier' (data field) | unique identifier of the originator of an electronic message (UIS) [22] | In the XXXXXXXXXX format | 'landlineNumber': '1212312345678', 'mobileNumber': '1212312345678', 'email': 'qwerty1@example.ru', | [0] |
| 2.5 | ʻactionStatus' (data field) | status of restriction on funds debiting | One code shall be selected from the limited set of possible values: • [on] – a request for the restriction in the form of a ban on debiting funds from bank (correspondent) accounts (sub-accounts); • [off] – a request to lift the restriction in the form of a ban on debiting funds from bank (correspondent) accounts (sub-accounts) | <pre>'position': 'position' }, 'attachment': { 'sourceld': 'f34030ef-358a-445c- 8567- 25985ce6d91c', 'comment': 'description of the attachment', 'dateTimeAt': '2018- 03-22T08:14:38Z', 'file': { 'name': 'file name', 'size': 'file size in bytes', 'base64': 'attachment in base64 format' } }</pre> | [0] |
| 2.6 | 'dateAt' | a calendar date from | data submission format | } }] } | [0] |

| | (data field) | which it is passage to | in accordance with ICO |
|-------|------------------------------|---|------------------------|
| | (data field) | which it is necessary to | in accordance with ISO |
| | | suspend the exchange of electronic messages | 8601:2004 [23] |
| | | when funds are | |
| | | transferred within the | |
| | | Bank of Russia payment | |
| | | system due to the | |
| | | identification of | |
| | | problems in providing | |
| | | information protection | |
| | | and making (suspicion | |
| | | about making) | |
| | | unauthorised money | |
| | | transfers | |
| 2.7 | 'text' | additional description | textarea (text field) |
| 20 | (data field) | identifiers of the resist of | |
| 2.8 | ʻperson' (data block) | identifiers of the point of contact who sent a | |
| | (uata DIOCK) | request to impose or lift | |
| | | the restriction in the | |
| | | form of a ban on debiting | |
| | | funds to bank | |
| | | (correspondent) accounts | |
| | | (sub-accounts) | |
| 2.8.1 | 'lastName' | surname | textarea (text field) |
| | (data field) | | |
| 2.8.2 | 'firstName' | name | textarea (text field) |
| | (data field) | | |
| 2.8.3 | ʻmiddleName' (data field) | middle name | textarea (text field) |
| 2.8.4 | 'landlineNumber' | stationary phone | textarea (text field) |
| 2.0.4 | (data field) | stationary phone | textarea (text field) |
| 2.8.5 | 'mobileNumber' | mobile phone | textarea (text field) |
| | (data field) | | |
| 2.8.6 | 'email' | e-mail address | textarea (text field) |
| | (data field) | | |
| 2.8.7 | 'position' | position | textarea (text field) |
| | (data field) | | |
| 2.9 | 'attachment' | additional data to | |
| | (data block) | confirm the | |
| | | imposition or lift of the | |
| | | restriction in the form of a | |

| | | ban on debiting funds | |
|-------|------------------------------|--|---|
| 2.9.1 | ʻsourceld' (data field) | identifier assigned by an information exchange participant | 128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by an information exchange participant |
| 2.9.2 | 'comment' (data field) | attachment description | textarea (text field) |
| 2.9.3 | 'dateTimeAt' (data field) | date and time when the file was added | data provision format in accordance with Specification RFC 3339 [11] |
| 2.9.4 | 'file' (data block) | data file | Specify the name and size of the file (no more than 5 MB) and perform Base64 encoding |

11. The form of an information message of the Bank of Russia on imposing (or lifting) the restriction on bank (correspondent) accounts (sub-accounts) of information exchange participants in the form of a ban on debiting funds

The form of an information message of the Bank of Russia on imposing (or lifting) the restriction on the bank (correspondent) accounts (sub-accounts) of information exchange participants in the form of a ban to debit funds shall be used as follows:

when sending a notification to an information exchange participant in the event of achieving a positive result of integrity control and acceptance of requests to impose or lift the restriction in the form of a ban to debit funds [21];

when sending a notification to an information exchange participant in the event of achievement of a negative result of integrity control and non-acceptance of requests to impose or lift the restriction in the form of a ban on funds debiting [21].

11.1. Identification data of an information message of the Bank of Russia on imposing (or lifting) the restriction on bank (correspondent) accounts (sub-accounts) of information exchange participants in the form of a ban on debiting funds. Data block **[HEADER]**

| Data block (field) No. | ldentifier of data block (field) | Data block (field) content | Data field format | E-mail format |
|---------------------------------|-------------------------------------|---|--|------------------------|
| 1.1 | ʻschemaType' (data field) | type of electronic message | Specify the value of [lockResponse] – an information message of the Bank of Russia on imposing (or lifting) the restriction on bank (correspondent) accounts (sub- accounts) of information exchange participants in the form of a ban on debiting funds | { |
| 1.2 | 'schemaVersion' (data field) | electronic message type scheme version | textarea (text field) | 02T15:00:00.05Z' }, |
| 1.3 | ʻversion' (data field) | electronic message version number during information exchange | numeric value (int) | |
| 1.4 | ʻmemberld' (data field) | identifier of an information exchange participant assigned by the Bank of Russia | 128-bit identifier (GUID) generated in accordance with RFC specification 4122 [16] assigned by the Bank of Russia | |

| 1.5 | ʻsourceld' (data field) | information exchange participant | 128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by the information exchange participant |
|-----|-------------------------------|-------------------------------------|--|
| 1.6 | ʻpublishedAt' (data field) | | data submission format in accordance with Specification RFC 3339 [11]. |

11.2. Description of the form of an information message of the Bank of Russia on imposing or lifting the restriction on the bank (correspondent) accounts (sub-accounts) of information exchange participants in the form of a ban to debit funds. Data block **[lockResponse]**

| Data block (field) No. | ldentifier of data block (field) | Data block (field) content | Data field format | E-mail format |
|---------------------------------|-------------------------------------|---|--|---|
| 2.1 | ʻsourceld' (data field) | identifier assigned by an information exchange participant | 128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by an information exchange participant | 'sourceld': 'f34030ef-358a-445c-8567-25985ce6d91c', |
| 2.2 | ʻorgBik' (data field) | BIC of an information exchange participant | in the AAAAAAAA format | 'coordinationStatus': 'the status of integrity control of a request to impose or lift the restriction in the form of a ban on debiting funds |
| 2.3 | ʻregNumber' (data field) | registration number from the register of state registration of credit institutions | textarea (text field) | 'dateAt': '20180101', 'text': 'additional description', 'attachment': { 'sourceId': 'f34030ef-358a-445c-8567- |
| 2.4 | ʻuniqldentifier' (data field) | unique identifier of the originator of an electronic message (UIS) [22] | In the XXXXXXXXXX format | 25985ce6d91c', 'comment': 'attachment description', 'dateTimeAt': '2018-03-22T08:14:38Z', 'file': { 'name': 'file name', |
| 2.5 | ʻactionStatus' (data field) | status of restriction on funds debiting | One code is selected from the limited set of possible values: [on] – a request for the restriction in the form of a ban on debiting funds from bank (correspondent) accounts (subaccounts); | 'size': 'file size in bytes', 'base64': 'attachment in base64 format' } |

| | | | • [off] – a request to lift the restriction in the form of a ban on debiting funds from bank (correspondent) accounts (sub-accounts) |
|-----|--|--|--|
| 2.6 | 'coordination Sta- tus' (data field) | the status of integrity control of a request to impose (or lift) the restriction on the bank (correspondent) accounts (sub-accounts) of information exchange participants in the form of a ban on debiting funds | One code is selected from the limited set of possible values: [accepted] – a positive result of integrity control and acceptance of the request for imposing (or lifting) the restriction in the form of a ban on debiting funds; [rejected] – a negative result of integrity control and non-acceptance of the request to impose (or lift) the restriction in the form of a ban on debiting funds |
| 2.7 | ʻdateAt' (поле данных) | calendar date from which it is necessary to cancel the suspension of the exchange of electronic messages when funds are transferred within the Bank of Russia payment system due to the identification of problems in providing information protection and making (suspicion about making) unauthorised money transfers | data submission format in accordance with ISO 8601:2004 [23] |
| 2.8 | 'text' (data field) | additional description | textarea (text field) |
| 2.9 | 'attachment' | additional data | |

| | (data block) | containing information on transactions in bank (correspondent) accounts (sub-accounts) of an information exchange participant | |
|-------|------------------------------|--|---|
| 2.9.1 | ʻsourceld' (data field) | identifier assigned by an information exchange participant | 128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by an information exchange participant |
| 2.9.2 | 'comment' (data field) | attachment description | textarea (text field) |
| 2.9.3 | 'dateTimeAt' (data field) | date and time when the file was added | data provision format in accordance with Specification RFC 3339[11] |
| 2.9.4 | 'file' (data block) | data file | Specify the name and size of the file (no more than 5 MB) and perform Base64 encoding |

12. The form of distribution by the Bank of Russia among information exchange participants of data on the detected incidents associated with violations of data protection requirements

| Data block (field) No. | ldentifier of data block (field) | Data block (field) content | Data field format | E-mail format |
|---------------------------------|-------------------------------------|---|---|--|
| 1.1 | 'schemaType' | type of electronic | Specify [REACTION] value – | { |
| | (data field) | message | Bank of Russia Information Bulletin | <pre>'header': {</pre> |
| 1.2 | 'schemaVersion' (data field) | electronic message type scheme version | textarea (text field) | 'schemaVersion': '1', 'version': '1', |
| 1.3 | ʻversion' (data field) | electronic message version number during exchange participant | numeric value (int) | 'publishedAt': '2002-10-02T15:00:00.05Z' }, |
| 1.4 | ʻpublishedAt' (data field) | date and time of information provision | data submission format in accordance with Specification RFC 3339 [11] | |

12.1. Information bulletin identification data. Data block **[HEADER]**

12.2. Description of the form of the information bulletin. Data block **[REACTION]**

| Data block (field) No. | ldentifier of data block (field) | Data block (field) content | Data field format | E-mail format |
|---------------------------------|-------------------------------------|-------------------------------|---------------------------------------|---|
| 1.1 | 'fixationAt' | date and time of the | data provision format in accordance | 'reaction': { |
| | (data field) | incident with an | with Specification RFC 3339[11] | 'fixationAt': '2002-10-02T15:00:00.05Z', |
| | | information exchange | | 'rootCause': 'key causes of the incident', 'vectorCode': |
| | | participant | | <pre>'computer attack vector identifier', 'serviceType': [{</pre> |
| 1.2 | 'rootCause' | key causes of the | textarea (text field) | 'type': 'type of attacked object', |
| | (data field) | incident | | 'name': 'name of software/hardware', |
| 1.3 | 'vectorCode' | computer attack vector | One code is selected from the limited | - |
| | (data field) | identifier | set of possible values: | 'version': 'version of software/hardware', |
| | | | vector [INT] – aimed at | - |

| | | | the infrastructure of an information | 'description': 'additional description of the type of |
|-------|----------------|----------------------------|---|---|
| | | | exchange participant; | object under attack' |
| | | | vector [EXT] – aimed at | }], |
| | | | an information exchange | 'typeOfAttack': 'computer attack type code', |
| | | | participant's customer; | ;antifraudDistribution': [{ |
| 1.4 | 'serviceType'(| identifier of an | If it is necessary to specify several | 'device': { |
| | data block) | information infrastructure | data field values (type, name, version, | ʻip': '127.0.0.1', |
| | | object | description), specify one or several | 'imsi': 'international mobile subscriber |
| | | | objects in the data block | identifier (individual subscriber number)', |
| | | | 'serviceType" | 'imei': 'international mobile |
| 1.4.1 | 'type' | type of the object under | One code should be selected from the | equipment identifier', |
| | (data field) | attack | limited set of possible values: | 'aiic': 'acquiring institution identification coo |
| | (uutu neiu) | uttuck | • | (32 field ISO 8583)', |
| | | | 1) system levels: | 'cati': 'card acceptor terminal identification |
| | | | • [hw] – hardware, | (41 |
| | | | • [net] – network equipment, | field ISO 8583)', |
| | | | • [net _ s] – network | 'caic': 'card acceptor identification code (42 |
| | | | applications and services, | field ISO 8583)' |
| | | | • [hw _ s] – server components | }, |
| | | | of virtualisation, software | 'payee': { |
| | | | infrastructure services, | 'bik': '123456789', |
| | | | [os] – operating systems, | 'hash': |
| | | | database management systems, | 'P79969612A71BAB224C7CB534FD7A0D3C1C78AD40664C48F12A9AE48FA |
| | | | application servers; | 11', |
| | | | | 'hashSnils': |
| | | | 2) the level of the AS and | 'B49087832A71BAB224C7CB534FD7A0D3C1C78AD40664C48F12A9AE48FA |
| | | | applications used to provide services | 44', |
| | | | within the framework of business or | (inn': '123456789000', |
| | | | technological processes of an | 'transferId': { |
| | | | information exchange participant: | 'paymentCard': { |
| | | | . | 'number': |
| | | | • [rbs] – remote banking system, | '123412341234123412' |
| | | | • [front-office] – payment card | }, |
| | | | transaction processing system, | 'settlement': { |
| | | | • [web] – information resources | 'number': |
| | | | of the Internet, | '12345123451234512345' |
| | | | • [abs] – automated banking | }, |
| | | | system, | 'phoneNumber': { |
| | | | • [back-office] – a system of | 'number': '1212312345678' |
| | | | | }, |
| | | | | ʻidNumber': { |
| | | | | 'number': |

| | | | post-transaction servicing of transactions carried out using payment cards; [participant _ w] – automated systems used by employees of an information exchange participant 3) the level of the AC and applications of the information exchange participant's customer: [cfs] – file server, [crbs] – remote banking system, [ecs] – e-mail server; [client_w] – automated systems used by employees of an information exchange participant's client; 4) other system: [oth] – other system | <pre>'1KoX6AA5VTdbBTkw27YEqKFaTtEQq97AAT'</pre> |
|-------|--------------------------------|---|--|---|
| 1.4.2 | 'name' (data field) | name of software/hardware | textarea (text field) | |
| 1.4.3 | 'version' (data field) | version of software- /hardware information | textarea (text field) | |
| 1.4.4 | 'description' (data field) | additional description of the type of the object under attack | textarea (text field) | |
| 1.5 | 'typeOfAttack' (data field) | computer attack type identifier | One code is selected from a limited set of possible values: [trafficHijackAttacks] – computer attacks related to changes in route and address information; [malware] – computer attacks related to the use of | |



| [sim] – computer attacks | |
|---|--|
| associated with the change | |
| (substitution) of the mobile | |
| subscriber identifier (IMSI) of the SIM | |
| card number, as well as with the | |
| replacement of the mobile | |
| equipment identifier (IMEI); | |
| [phishingAttacks] – computer | |
| attacks related to information that | |
| misleads information exchange | |
| participants and their clients, as well | |
| as other persons interacting with | |
| them, about the ownership of the | |
| information disseminated via the | |
| Internet due to the similarity of | |
| domain names, design or content. | |
| [prohibitedContents] – | |
| computer attacks related to the | |
| distribution of information related to | |
| the offer and/or provision of financial | |
| services in the Russian Federation by | |
| persons not authorised to do so in | |
| accordance with the legislation of the | |
| Russian Federation. Posting | |
| prohibited content on the Internet; | |
| • [[maliciousResources] – | |
| computer attacks related to the | |
| placement on the Internet of | |
| information enabling illegal access to | |
| information systems of information | |
| exchange participants and their | |
| customers used when providing | |
| (buying) financial services, including | |
| through illegal access to confidential | |
| customer information. | |
| | |
| | |
| | |
| | |
| | |

| | | | Placing a malicious resource on the Internet; [changeContent] – computer attacks related to changes in content; [scanPorts] – computer attacks related to scanning software ports of information infrastructure objects of information exchange participants by persons who do not have the relevant authority; [other] – other computer attacks against information infrastructure objects of information exchange participants and their clients |
|-------|---|--|---|
| | ʻantifraudDistribut ion' (data block) | | If it is necessary to specify several data field values (device, payee, additionalStatus), specify one or several objects in the data block 'antifraudDistribution' |
| 1.6 | 'device' (data subblock) | identifiers of the device used for conducting an unauthorised transaction | |
| 1.6.1 | 'ip' (data field) | | Logical IPv4 address shall comply with Specification RFC 791 [12] |
| 1.6.2 | 'imsi' (data field) | International Mobile Subscriber Identity (IMSI) means the international identifier of a mobile subscriber (individual number of a subscriber (individual customer) by which the system recognises a mobile communication user applying GSM and UMTS standards | number (15-bit in decimal) AA- BBBBBB-CCCCCC-EE |

| [] | | | |
|-------|------------------------|---|--|
| | | | |
| | | | |
| 1.6.3 | 'imei' (data field) | International Mobile Equipment Identity (IMEI) – the international identifier of mobile equipment (mobile device of an individual customer) | number (15-bit in decimal) AA- BBBBBB-CCCCCC-EE |
| 1.6.4 | ʻaiic' (data field) | identifier of the participant who is an acquiring bank when it transfers funds using payment cards | identifier of the participant who is an acquiring bank in the course of money transfer operations using payment cards (Acquiring institution identification code) - field 'F032' of ISO 8583 Financial Messaging Standard [7], [8], [9] |
| 1.6.5 | 'cati' (data field) | identifier of the ATM and/or the electronic terminal where funds are transferred and/or withdrawn | identifier of the ATM and/or electronic terminal where the funds are transferred and/or withdrawn (Card acceptor identification code), – field 'F041'* of ISO 8583 Financial Messaging Standard [7], [8], [9] * The terminal identifier value should be aligned to the left and |
| | | | supplemented with spaces on the right with up to 8 characters |
| 1.6.6 | 'caic' (data field) | identifier of the ATM and/or electronic terminal where funds are transferred and/or withdrawn by its geographical location | identifier of the ATM and/or electronic terminal where funds are transferred and/or withdrawn by its geographical location (Card acceptor identification code) – field 'F042'* of ISO 8583 Financial Messaging Standard [7], [8], [9] |

| | | | * The value of the service point identifier shall be aligned to the left and supplemented with spaces on the right with up to 15 characters |
|-------|-------------------------|---|---|
| 1.7 | 'payee' (data block) | information determining the payee when funds are transferred without the customer's consent (hereinafter, information on the payee) | |
| 1.7.1 | 'bik' (data field) | BIC of the money transfer operator serving the payee | in the AAAAAAAA format |
| 1.7.2 | ʻhash' (data field) | sequence of symbols obtained as a result of calculating the SHA-256 hash function from the identification document series and number | The sequence of symbols obtained as a result of the calculation of the SHA-256 hash function from the identification document series and number. The series and number of the identification document are provided for calculating a hash function: without spaces (_), the number sign (N), letters (if any) in upper register (ABC). For the Russian passport this is XXXXYYYYYY , where: XXXX is four-digit passport series; YYYYYY is a six-digit passport number. Source text encoding (before hash) - Windows-1251; Hash text encoding – Windows-1251. |

| 1.7.3 | 'hashSnils' | SNILS number as the SHA- | · · · · · |
|----------|-----------------|--|--|
| | (data field) | 256 hash function | a result of calculating the SHA-256 hash function from the payer SNILS. |
| | | | |
| | | | SNILS is provided for calculating a hash function: without spaces () and |
| | | | separation marks (-). |
| | | | SNILS type: XXXXXXXXXXXX |
| | | | Source text encoding (before hash) - Windows-1251; |
| | | | Hash text encoding – Windows-1251. |
| 1.7.4 | 'inn' (data | TIN of the payee - a legal | In the XXXXXXXXXX format – for |
| 1.7.1 | field) | entity | legal entities, in XXXXXXXXXX or |
| | | | XXXXXXXXX formats – for individual entrepreneurs and (or) |
| | | | individuals engaged in private businesses in accordance with the |
| | | | procedure established by the |
| 1.7.5 | 'transferId' | identification data | legislation of the Russian Federation |
| 1.7.5 | (data subblock) | depending on the money transfer method | |
| 1.7.5.1 | 'paymentCard' | | If it is necessary to specify several |
| | (data subblock) | using payment cards | values of data blocks (number), specify one or several objects in the |
| | | | data block 'paymentCard' |
| 1.7.5.1. | 'number' | number of the payment | in the XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX |
| 1 | (data field) | card of the payee issued to him/her and (or) the | format |
| | | person authorised by the payee, by the money | payment card number shall be |
| | | transfer operator – the issuer | provided without spaces (_) and separation marks (-). |
| 1.7.5.2 | 'settlement' | when making money | If it is necessary to specify |

| | (data sub-block) | transfers in bank | several values of the data field |
|----------|------------------|-----------------------------|---|
| | | accounts by debiting | (number), specify one or several |
| | | | objects in the 'settlement' data sub- |
| | | accounts | block |
| | | | |
| 1.7.5.2. | 'number' | the settlement account | in the |
| 1 | (data field) | number of the payee | XXXXXXXXXXXXXXXXXXXXXXXX |
| | | opened with the money | format |
| | | transfer operator | |
| | | serving the payee | bank account number shall be |
| | | | provided without spaces (_) and |
| 1.7.5.3 | 'phoneNumber' | when making money | separation marks (-). If it is necessary to specify an |
| 1.7.5.5 | (data subblock) | transfers by telephone | additional value of the data field |
| | | number | (number), specify one or more objects |
| | | | in the data sub-block 'phoneNumber" |
| | | | |
| 1.7.5.3. | 'number' | telephone number of the | In the KKKXXXNNNNNNN |
| 1 | (data field) | payee | format, where: |
| | | | KKK – a country code of one to three |
| | | | characters; |
| | | | XXX – operator's code; |
| | | | NNNNNN - seven characters of the |
| | | | number. |
| | | | |
| | | | The telephone number shall be |
| | | | provided without a plus sign (+), |
| | <i>(</i> | | spaces (_) and separation signs (-). |
| 1.7.5.4 | 'idNumber' | if the balance of | If it is necessary to specify an |
| | (data subblock) | electronic funds changes | additional value of the data field (number), specify one or more objects |
| | | changes | in the data sub-block 'idNumber' |
| | | | |
| 1.7.5.4. | 'number' | identification number of | textarea (text field) |
| 1 | (data field) | the payee, in particular, | , , , , |
| | | the number of the | |
| | | electronic wallet of the | |
| | | payee used by him on the | |
| | | basis of a bank account | |
| | | | |

| | | agreement and (or) an agreement on the use of the electronic means of payment concluded with the money transfer operator | |
|-----|---|---|--|
| 1.8 | ʻcrossBorder' (data field) | cross-border banking identifier | One code is selected from the limited set of possible values: [CRB] – cross-border transfer; [DOM] – domestic transfer |
| 1.9 | 'additionalTransa tionApprove' (data field) | identifier of additional transaction confirmation | One or more codes shall be selected from the limited set of possible values: • [3DS] – an operation was confirmed using 3D Secure; • [DCS] – implementation of technological measures to use separate technologies [3]; • [NAA] – an operation without confirmation; • [SMS] – an operation was confirmed using short text messages (SMS); • [LTR] – an operation was performed in accordance with the list of trusted payees; • [TEL] – an operation was confirmed by telephone; • [OAA] – other confirmation method |

12.3. Information on technical data describing computer attacks against information infrastructure facilities of information exchange participants and their customers, as well as on relevant forms of electronic messages. Data Block **[IMPACTS]**

12.3.1. Computer attacks related to changes in route and address information [trafficHijackAttacks] (for [INT], [EXT] vector)

| Data block (field) No. | Data block (field) identifier | Data block (field) content | Data field format | E-mail format |
|---------------------------------|-------------------------------------|---|-----------------------|--|
| 1.1 | ʻlegalAsPath' (data field) | Legal AS-Path | textarea (text field) | 'impacts': { |
| 1.2 | ʻwrongAsPath' (data field) | Wrong AS-Path | textarea (text field) | <pre>'legalAsPath': 'Legal As-Path', 'wrongAsPath': 'wrongAsPath':</pre> |
| 1.3 | 'lookingGlass' (data field) | Reference to the Looking Glass used to verify AS-Path | textarea (text field) | 'lookingGlass': 'Reference to the Looking Glass used to verify AS-Path', 'legalPrefix': 'Legal prefix', 'wrongPrefix': |
| 1.4 | ʻlegalPrefix' (data field) | Legal prefix | textarea (text field) | 'wrongPrefix' }], |
| 1.5 | ʻwrongPrefix' (data field) | Wrong prefix | textarea (text field) | |

12.3.2. Computer attacks related to the use of malicious software at information infrastructure facilities of information exchange participants and their clients **[malware]** (for [INT], [EXT] vector)

| Data block (field) No. | ldentifier of data block (field) | Data block (field) content | Data field format | E-mail format |
|---------------------------------|-------------------------------------|-------------------------------|---|---|
| 2.2 | 'sources' | identifiers of sources of | If it is necessary to specify several | 'malware': [{ |
| | (data block) | malicious resources on | data field values (ip, domain, url), | 'sources': [{ |
| | | the Internet with which | specify one or several objects in the | 'ip': '127.0.0.1', |
| | | the attacked | data block 'sources'. | 'domain': 'example.com', |
| | | object interacts | | 'url': 'http://example.com' |
| 2.2.1 | 'ip' | IP address | Logical IPv4 address shall comply with | }], |
| | (data field) | | Specification RFC 791 [12] | 'classifications': [{ |
| | | | | 'vendorName': 'the name of the |
| 2.2.2 | 'domain' (data field) | domain name | Domain name according to Specification RFC 1034 [14] and the international hierarchy of domain zones according to Specification RFC 5890 [13] | MCSE tool used by the information exchange participant', 'vendorVerdict': 'MC class in accordance with the MCSE tool used by the information exchange participant' |

| | | | | }], |
|---------|-----------------------|---------------------------|---|--|
| | | | | 'malwareSamples': [{ |
| 2.2.3 | ʻurl' (data field) | URL-address | URL in accordance with Specification RFC 3986 [15] | 'hash': { 'md5': |
| 2.3 | 'classifications' | classification of | If it is necessary to specify several | '4BA5139A444538479D9D750E2E2779BF', |
| | (data block) | malicious code | data field values (vendorName, | 'sha1': |
| | (, | | vendorVerdict), specify one or | ' D2B063763378A8CB38B192B2F71E78BC13783EFE ', |
| | | | several objects in the | 'sha256': ' |
| | | | data block 'classifications' | E25059612A71BAB224C7CB438FD7A0D3C1C78AD40664C48F12A9AE48FA44 |
| 2.3.1 | 'vendorName' | name of the MCSE tool | textarea (text field) | 44' |
| | (data field) | used by an information | | }, |
| | (, | exchange participant | | ······································ |
| | | evena8e participant | | 'sourceld': 'f34030ef-358a- |
| 2.3.2 | 'vendorVerdict' | MC class in accordance | textarea (text field) | 445c-8567-25985ce6d91c', |
| | (data field) | with the MCSE tool used | (| 'comment': 'comment to |
| | (| by an information | | the attachment', |
| | | exchange participant | | 'dateTimeAt': '2018-03- |
| 2.4 | 'malwareSamples | | If it is necessary to specify several | 22T08:14:38Z', |
| | (data block) | | values of data sub-blocks (hash, | 'file': { |
| | (data biotity | | attachment), specify one or several | 'name': 'file name', |
| | | | objects in the data block | 'size': 'file size in |
| | | | 'malwareSamples' | bytes', |
| 2.4.1 | 'hash' | MC sample as hash | | 'base64': 'attachment |
| | (data subblock) | functions (hash functions | | in |
| | | MD5, SHA-1, SHA-256 are | | base64 format' |
| | | calculated for each MC | | }. |
| | | sample) | | 'fileLink': |
| | | 17 | | 'http://domain.com/archive.rar' |
| 2.4.1.1 | 'md5' | MC sample as the MD5 | The sequence of symbols obtained as | } |
| | (data field) | hash function | a result of calculating the MD5 hash | }], |
| | | | function | 'malwareMessageSenders': [{ |
| 2.4.1.2 | 'sha1' | MC sample as the SHA-1 | The sequence of symbols obtained as | 'email': 'qwerty@example.ru', |
| | (data field) | | a result of calculating the SHA-1 hash | 'server': '127.0.0.1' |
| | . , | | function | }], |
| 2.4.1.3 | 'sha256' | MC sample as the SHA- | The sequence of symbols obtained as | 'malwareMessageAttachment': { |
| | (data field) | | a result of calculating the SHA-256 | 'sourceld': 'f34030ef-358a-445c- |
| | . , | | hash function | 8567- |
| 2.4.2 | 'attachment' | MC sample as a file | | 25985ce6d91c', |
| | (data sub-block) | | | 'comment': 'comment to |
| 2.4.2.1 | (| identifier assigned by an | 128-bit identifier (GUID) generated in | attachment', 'dateTimeAt': '2018-03- |
| | 'sourceld' | information exchange | accordance with Specification RFC | 22T08:14:38Z', |
| | (data field) | participant | 4122 [16] | 'file': { |
| | | | - | 'name': 'file name', |
| | | | | , |

| | | | assigned by the information | bytes', | |
|----------|---|---|---|---|---|
| | | | exchange participant | - | 'base64': 'attachment in |
| 2.4.2.2 | 'comment' (data field) | attachment description | textarea (text field) | base64 format' | }, 'fileLink': |
| 2.4.2.3 | 'dateTimeAt' (data field) | date and time when the file was added | data submission format in accordance with Specification RFC 3339 [11] | http://domain.com/archive.rar }, | armfulResourceAddress': [{ 'ip': |
| 2.4.2.4. | 'file' (data | additional materials | Specify the name and size of the file | - | '127.0.0.1', |
| 1 | subblock) | containing MC samples | (no more than 5 MB) and perform Base64 encoding | | 'domain': 'example.com', 'url': 'http://example.com' |
| 2.4.2.5 | 'fileLink' (data field) | additional materials containing MC samples | Specify the URL for downloading the file, if its size exceeds 5 MB, in accordance with Specification RFC 3986 [15] | }], ′io | |
| 2.5 | 'malwareMessage Senders' (data block) | mailboxes from which a | If it is necessary to specify several data field values (email, server), specify one or several objects in the data block 'malwareMessage' | compromising identifier', description' | 'comment': 'additional }], |
| 2.5.1 | ʻemail' (data field) | sender's e-mail address | The sender's e-mail address shall be submitted in the format in accordance with Specification RFC 5322 [18] | compromising identifier', | 'fil': [{ 'impact': 'type of detected 'comment': 'additional |
| 2.5.2 | 'server' (data field) | IP address of the last mail server | Logical IPv4 address shall comply with Specification RFC 791 [12] | | }], 'reg': [{ 'import', (type of detected |
| 2.6 | malwareMessage- Attachment (data sub-block) | source code file of an e- mail (if an MC was sent to an e-mail box) | | compromising identifier', description' | 'impact': 'type of detected 'comment': 'additional }], (agg/c [[|
| 2.6.1 | ʻsourceld' (data field) | | 128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by the information exchange participant | compromising identifier', description' | 'prc': [{ 'impact': 'type of detected 'comment': 'additional }], |
| 2.6.2 | 'comment' (data field) | attachment description | textarea (text field) | | 'oth': [{ 'impact': 'type of detected |
| 2.6.3 | 'dateTimeAt' (data field) | date and time when the file was added | data submission format in accordance with Specification RFC 3339 [11] | compromising identifier', | 'comment': 'additional |

| 2.6.4.1 | 'file' (data | data file containing sn | Specify the name and size of the file | description' | | |
|---------|--|--|---|--------------|----------|--|
| | block) | MC sample | (no more than 5 MB) and perform Base64 encoding | | }], | 3] |
| 2.6.4.2 | 'fileLink' (data field) | link for obtaining (downloading) a data file containing MC samples | Specify the URL for downloading the file, if its size exceeds 5 MB, in accordance with Specification RFC 3986 [15] | | ʻinfecti | onMethod': [{ 'type': 'type of probable infection method', |
| 2.7 | 'harmfulResourc e- Address' (data block) | identifiers of a malicious resource from which the MC was downloaded | If it is necessary to specify several data field values (ip, domain, url), specify one or several objects in the data block 'sources.' 'harmfulResourceAddress' | type' }], | }] | 'comment': 'comment to the selected |
| 2.7.1 | 'ip' (data field) | IP address | Logical IPv4 address shall comply with Specification RFC 791 [12] | | | |
| 2.7.2 | 'domain' (data field) | domain name | Domain name according to RFC 1034 specification [14] and the international hierarchy of domain zones according to Specification RFC 5890 [13] | | | |
| 2.7.3 | ʻurl' (data field) | URL-address | URL in accordance with Specification RFC 3986 [15] | - | | |
| 2.8 | 'iocs' (data block) | identified compromise indicators | If it is necessary to specify several values of data fields (net, fil, reg, prc, oth), specify one or several objects in the 'iocs' data block | | | |
| 2.8.1 | 'net' (data subblock) | network indicators | If it is necessary to specify several values of data fields (impact, comment), specify one or several objects in the 'net' data block | | | |
| 2.8.1.1 | 'impact' (data field) | type of compromising identifier detected | One code is selected from the limited set of possible values: • [CRT] – creation of technical data; • [UPD] – change in technical data; • [DLT] – technical data deletion | | | |

| | | | - |
|---------|---------------------------|---|--|
| 2.8.1.2 | 'comment' (data field) | additional description | textarea (text field) |
| 2.8.2 | ʻfil' (data sub-block) | file indicators | If it is necessary to specify several values of data fields (impact, comment), specify one or several objects in the 'fil' data sub-block |
| 2.8.2.1 | 'impact' (data field) | type of compromising identifier detected | One code is selected from the limited set of possible values: • [CRT] – creation of technical data; • [UPD] – change in technical data; • [DLT] – technical data deletion |
| 2.8.2.2 | 'comment' (data field) | additional description | textarea (text field) |
| 2.8.3 | ʻregʻ (data sub-block) | OS register indicators | If it is necessary to specify several values of data fields (impact, comment), specify one or several objects in the 'reg' data block |
| 2.8.3.1 | 'impact' (data field) | type of compromising identifier detected | One code is selected from the limited set of possible values: [CRT] – creation of technical data; [UPD] – change in technical data; [DLT] – technical data deletion |
| 2.8.3.2 | 'comment' (data field) | additional description | textarea (text field) |
| 2.8.4 | ʻprc' (data sub-block) | indicators of OS processes | If it is necessary to specify several values of data fields (impact, comment), specify one or several objects in the 'prc' data sub-block |
| | | 1 |
|---------------------------|---|--|
| 'impact' (data field) | type of compromising identifier detected | One code is selected from the limited set of possible values: |
| | | • [CRT] – creation of |
| | | technical data; |
| | | • [UPD] – change in technical |
| | | data; |
| | | • [DLT] – technical data deletion |
| 'comment' (data field) | additional description | textarea (text field) |
| | | If it is necessary to specify several |
| sub-block) | | values of data fields (impact, |
| | | comment), specify one or several objects in the 'oth' data sub-block |
| | | |
| 'impact' | type of compromising | One code is selected from the limited |
| (data field) | identifier detected | set of possible values: |
| | | • [CRT] – creation of |
| | | technical data; |
| | | • [UPD] – change in technical |
| | | data; |
| | | • [DLT] – technical data deletion |
| 'comment' | additional description | textarea (text field) |
| <u> </u> | identifier of the accurace | If it is necessary to specify several |
| | method of 'infection' | values of data fields (type, comment), |
| (uutu biotity | | specify one or several objects in the |
| | | data block 'infectionMethod' |
| 'type' | type of probable | One code is selected from the limited |
| (data field) | infection method | set of possible values: |
| | | • [EML] – via e-mail channels; |
| | | [EWL] – Via e-mail channels; [DSD] – from a storage medium; |
| | | [LCL] – distributed via a |
| | | |
| | 'comment' (data field) 'oth' (data sub-block) 'impact' (data field) 'infectionMethod' (data block) 'type' | (data field)identifier detected'comment' (data field)additional description'oth' (data sub-block)indicators not included in (2.8.1 - 2.8.4.2.)'impact' (data field)type of compromising identifier detected'impact' (data field)type of compromising identifier detected'comment' (data field)additional description identifier of the assumed method of 'infection''type'type of probable |

| | | | local network; |
|-------|--------------|-------------------------|------------------------|
| | | | • [OTH] – other method |
| 2.9.2 | 'comment' | comment to the selected | textarea (text field) |
| | (data field) | type | |

12.3.3. Computer attacks that have been launched as a result of inducing clients to conduct money transfer transactions through deception or abuse of trust **[socialEngineering]** (for [EXT] vector)

| | - | | | |
|---------------------------------|-------------------------------------|---|---|--|
| Data block (field) No. | ldentifier of data block (field) | Data block (field) content | Data field format | E-mail format |
| 3.1 | 'soiTypes' (data field) | social engineering method identifiers | One or more codes shall be selected from the limited set of possible values: [MOB] – a call from a mobile telephone number; [TPH] – a call from a telephone number starting with 8-800; [SMS] – an SMS message; [SNW] – social engineering using social networks; [MSG] – social engineering using instant messaging tools; [OTH] – another way to implement social engineering methods | 'socialEngineering': { 'soiTypes': ['identifiers of social engineering methods'] 'soiSenders': [{ 'phoneNumber': '1212312345678', 'phoneNumber': '1212312345678', 'email': 'qwerty@yandex.ru', 'server': '127.0.0.1']], 'messageAttachment': { 'sourceld': 'f34030ef-358a- 445c- 8567-25985ce6d91c', 'comment': 'attachment description', 'datetimeAt': |
| 3.2 | 'soiSenders' (data block) | social engineering implementation identifiers | If it is necessary to specify several data field values (phoneNumber, email, server), specify one or several objects in the data block 'soiSenders' | 22T08:14:38Z', 'file': { |
| 3.2.1 | 'phoneNumber' (data field) | telephone number | in the KKKXXXNNNNNNN format, where: KKK – a country code of one to three characters; XXX – operator's code; NNNNNNN - seven characters of the number. A telephone number shall be provided without | 'base64': 'attachment in base64 format' }, 'fileLink': 'http://domain.com/archive.rar' }, 'description': 'additional description' }, |

STO BR BFBO-1.5-

| | | | a plus sign (+), spaces (_) and |
|---------|------------------|---------------------------|---|
| | | | separation signs (-). |
| 3.2.2 | 'email' | e-mail address | The sender's e-mail address shall be |
| - | (data field) | | provided in the format in accordance |
| | (, | | with RFC 5322 specification [18] |
| | | | · · · · · · · · · · · · · · · · · · · |
| 3.2.3 | 'server' | IP address of the last | Logical IPv4 address shall comply with |
| | (data field) | mail server | RFC 791 specification [12] |
| 3.3 | 'message Attach- | data files describing the | , |
| 5.5 | ment' | social | |
| | (data block) | engineering method | |
| 3.3.1 | (1.0.00.0.00.0.) | | 128-bit identifier (GUID) generated in |
| 5.5.1 | | identifier assigned by an | accordance with RFC 4122 |
| | 'sourceld' | information exchange | specification [16] assigned by the |
| | (data field) | participant | information exchange participant |
| | | purclopurc | |
| 3.3.2 | 'comment' | | |
| | (data field) | attachment description | textarea (text field) |
| 3.3.3 | 'dateTimeAt' | date and time when the | data presentation format in accordance |
| | (data field) | file was added | with RFC 3339 specification [11] |
| | | | |
| 3.3.4.1 | 'file' (data | data files describing the | Specify the name and size of the file |
| | subblock) | social | (no more than 5 MB) and perform |
| | | engineering method | Base64 encoding |
| 3.3.5 | 'fileLink' | data files describing the | Specify the URL for downloading the file, |
| | (data field) | social engineering method | if its size exceeds 5 MB, in accordance |
| | | | with RFC 3986 specification [15] |
| | | | |
| 3.4 | 'description' | additional description | textarea (text field) |
| | (data field) | | |

12.3.4. Denial of service computer attacks (DDoS attacks) in relation to the information infrastructure of information exchange

participants [ddosAttacks] (for [INT] vector)

| Data bloc k (field) numb er | ldentifier of data block (field) | Content of data block (field) | Data field format | E-mail format |
|--|--|----------------------------------|---|--|
| 4.2 | ʻattackType' (data block) | attack type | | 'ddosAttacks': [{ |
| 4.2.1 | 'type' (data field) | attack type (by OSI levels) | One code shall be selected from the limited set of possible values: | 'type': 'type of attack (by OSI levels)', 'comment': 'additional description' |

| | [1]- 'L2/3: ICMP-flood', [2]- 'L2/3: NTP-amplification', [3]- 'L2/3: SENTINEL-amplification', [4]- 'L2/3: SENTINEL-amplification', [5]- 'L2/3: SNMP-amplification', [6]- 'L2/3: SSDP-amplification', [7]- 'L2/3: SSDP-amplification', [8]- 'L2/3: CHARGEN-amplification', [9]- 'L2/3: RIPv1-amplification', [10]- 'L2/3: RIPv1-amplification', [11]- 'L2/3: QTPD-amplification', [12]- 'L2/3: Quake-amplification', [13]- 'L2/3: QUAke-amplification', [14]- 'L2/3: QUAke-amplification', [15]- 'L2/3: Not Paramplification', [16]- 'L2/3: NetBIOS-amplification', [16]- 'L2/3: Steam-amplification', [17]- 'L2/3: Steam-amplification', [19]- 'L3: DPI-attack', [20]- 'L4: TCP-ACK-attack', [21]- 'L4: TCP-ACK-attack', [23]- 'L4: Smurf-attack', [24]- 'L4: ICMP/UDP-frag', [25]- 'L4: TCP-frag', [26]- 'L4: TCP-frag', | 22T08:14:38Z', 'negativeImpact': { 'type': 'type of negative impact', 'comment': 'additional description' }], |
|--|---|--|
| | [24]– 'L4: ICMP/UDP-frag', | |

| | | | [29] – 'L7: DNS-flood', |
|-------|---------------------------|---|---|
| | | | [30] – 'L7: HTTP/S-flood', |
| | | | [31] – 'L7: FTP-flood', |
| | | | [32] – 'L7: SMTP-flood', |
| | | | [33]– 'L7: VoIP/SIP-attack', |
| | | | [34] – 'L7: POP3-flood', |
| | | | [35]– 'L7: SlowRate-attack,' |
| | | | [36] – 'other' |
| 4.2.2 | 'comment' (data field) | additional description | textarea (text field) |
| 4.3 | 'sources' | identifiers of attack | If it is necessary to specify several |
| | (data block) | sources | values of the data field (ip), specify one or several objects in the data |
| | | | block 'sources' |
| 4.3.1 | 'ip' (data | | Logical IPv4 address shall comply with |
| | field) | source (in case of a large number | Specification RFC 791 [12] |
| | | of computer attack | |
| | | sources in the block | |
| | | 'sources', the top 100 IP | |
| | | addresses of the attackers are specified, | |
| | | with the complete | |
| | | list attached in a text file) | |
| 4.4 | 'power' | attack power | |
| 4.4.1 | (data block) 'pps' | number of packets | Packets per second |
| 4.4.1 | (data field) | per second | |
| 4.4.2 | 'mps' | number of megabits | Megabit per second |
| | (data field) | per second | |
| 4.4.3 | 'rps' (data | number of requests | Request per second |
| - | | norcocond | |
| | field) | per second | |
| 4.5 | 'startTimeAt' | attack start time | data provision format in accordance |
| | , | · · · · · · · · · · · · · · · · · · · | data provision format in accordance with Specification RFC 3339 [11]. |
| | 'startTimeAt' | · · · · · · · · · · · · · · · · · · · | |

| | | | 3339 [11] |
|-------|----------------------------------|-----------------------------------|--|
| 4.7 | ʻnegativeImpact' (data block) | negative effect from an attack | |
| 4.7.1 | 'type' (data field) | type of negative impact | One code should be selected from the limited set of possible values: |
| | | | [NAW] – service availability interruption; [OTH] – service degradation; [NCQ] – service was not adversely affected |
| 4.7.2 | 'comment' (data field) | additional description | textarea (text field) |

12.3.5. Computer attacks related to unauthorised access to ATMs and payment terminals of information exchange participants [atmAttacks] (for [INT] vector)

| Data block (field) No. | ldentifier of data block (field) | Data block (field) content | Data field format | E-mail format |
|---------------------------------|-------------------------------------|---|---|---|
| 5.1 | 'target' (data block) | identifier of object to be attacked object | | <pre>'atmAttacks': {</pre> |
| 5.1.1 | 'type' (data field) | attacked object type | One code is selected from the limited set of possible values: [ATM] is an ATM; [CIN] is an ATM capable to accept cash; [REC] is an ATM with a recycling function; [POS] is a POS-terminal; [SST] is a payment terminal; [OTH] is other facility | object under attack', 'description': 'additional description', }, 'attackType': [{ 'type': 'type of attack depending on 'description'': 'additional description' }], 'attackImages': { 'sourceld': 'f34030ef-358a-445c-8567- |
| 5.1.2 | 'description' (data field) | additional description | textarea (text field) | 25985ce6d91c', 'comment': 'description of |
| 5.2 | 'attackType' (data block) | attack type | If it is necessary to specify several values of data fields (type, description), specify one or several objects in the data block 'sources' | attachment', 'dateTimeAt': '2018- 03-22T08:14:38Z', 'file': { 'name': 'file name', 'size': 'file size in bytes', |

| | | | - | | | 'base64': 'attachment in |
|---------|-------------------------------|---|---|----------------|---------|--|
| 5.2.1 | 'type' (data field) | type of attack depending on the target | One code is selected from the limited is set of possible values: • [BBX] – blackbox attacks; • [DSP] – 'direct dispense' attacks and their variations; • [SKM] – skimming; • [OTH] – other method | base64 format' | } }, | }, 'fileLink': 'http://domain.com/archive.rar' |
| 5.2.2 | 'description' (data field) | additional description | textarea (text field) | | | |
| 5.3 | attackImage (data block) | additional materials of attack launch | | | | |
| 5.3.1 | ʻsourceld' (data field) | identifier assigned by an information exchange | 128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by the information exchange participant | | | |
| 5.3.2 | 'comment' (data field) | attachment description | textarea (text field) | | | |
| 5.3.3 | 'dateTimeAt' (data field) | date and time when the file was added | data submission format in accordance with Specification RFC 3339 [11] | | | |
| 5.3.4.1 | 'file' (data subblock) | data file containing additional materials | Specify the name and size of the file (no more than 5 MB) and perform Base64 encoding | | | |
| 5.3.5 | 'fileLink' (data field) | (downloading) a data file containing | Specify the URL for downloading the file, if its size exceeds 5 MB, in accordance with Specification RFC 3986 [15] | | | |

12.3.6. Computer attacks related to information infrastructure vulnerabilities of information exchange participants and their clients **[vulnerabilities]** (for vector [INT], [EXT])

| Data block (field) No. | ldentifier of data block (field) | Data block (field) content | Data field format | E-mail format |
|---------------------------------|-------------------------------------|---|--|-----------------------|
| 6.2 | 'sources' (data block) | identifiers of sources exploiting vulnerability | If it is necessary to specify several values of data fields (ip, url), specify one or several objects in the data block 'sources' | 'vulnerabilities': [{ |

| | | | | 'url': 'http://example.com' }], |
|-------|------------------------------|--------------------------|--|--|
| 6.2.1 | 'ip' (data field) | IP address | Logical IPv4 address shall comply with Specification RFC 791 [12] | 'identifier': 'vulnerability identifier', 'CVSS': 'CVSS metrics' }], |
| 6.2.2 | 'url' (data field) | URL-address | URL in accordance with Specification RFC 3986 [15] | |
| 6.3 | 'identifier' (data field) | vulnerability identifier | If a vulnerability is detected, its type shall be specified in accordance with the classification of the FSTEC of Russia, CVE: • FSTEC of Russia - https://bdu.fstec.ru/ vul; • Common Vulnerabilities and Exposures (CVE) – https://cve.mitre.org/data/downloa ds/all items.html | |
| 6.4 | ʻCVSS' (data field) | CVSS metrics | Specify the CVSS v 3.0 (The Common Vulnerability Scoring System (CVSS) if < * > is defined. Specify the maximum possible number of metrics listed as follows: basic metrics, temporary metrics, context metrics, and environment metrics. If no metrics are specified, use the FSTEC of Russia calculator – https://bdu.fstec.ru/cvss3 | |

12.3.7. Computer attacks related to searching (hacking) and compromising authentication data (login) data

[bruteForces] (for [INT] vector)

| Data block (field) No. | Data block (field) identifier | Data block (field) content | Data field format | E-mail format |
|---------------------------------|-------------------------------------|-------------------------------------|--|------------------------------|
| 7.2 | 'sources' (data block) | identification of attack sources | If it is necessary to specify several values of the data field (ip), specify one or several objects in the data block 'sources' | <pre>'bruteForces': [{</pre> |
| 7.2.1 | ʻip' | IP address of the attack source | Logical IPv4 address shall | |

| (data field) | | comply with Specification RFC | |
|--------------|-----------------------------|-------------------------------|--|
| | (in the case of a large | 791 [12] | |
| | number of computer | | |
| | attack sources, the data | | |
| | block 'sources' shall | | |
| | contain the top 100 IP | | |
| | addresses of the attackers, | | |
| | with the complete list | | |
| | attached in a text file) | | |
| | | | |

12.3.8. Computer attacks related to spam mailings to information exchange participants and their clients [spams] (for

[INT], [EXT] vector)

| Data block (field) No. | ldentifier of data block (field) | Data block (field) content | Data field format | E-mail format |
|---------------------------------|-------------------------------------|--|---|---|
| 8.1 | ʻreceivedAt' (data field) | date and time when a spam message was received | data submission format in accordance with Specification RFC 3339 [11] | 'spams': [{ |
| 8.2 | ʻsources' (data block) | attack source identifiers (spam senders) | If it is necessary to specify several data field values (ip, domain, email), specify one or several objects in the data block 'sources' | 'ip': '127.0.0.1', 'domain': 'example.com', 'email': 'qwerty@example.ru' }], 'spamImages': { |
| 8.2.1 | 'ip' (data field) | IP address | Logical IPv4 address shall comply with Specification RFC 791 [12] | 'sourceld': 'f34030ef-358a-445c- 8567- 25985ce6d91c', |
| 8.2.2. | 'domain' (data field) | domain name | Domain name according to RFC 1034 specification [14] and the international hierarchy of domain zones according to Specification RFC 5890 [13] | 'comment': 'comment to attachment', 'dateTimeAt': '2018-03- 22T08:14:38Z', 'file': { 'name': 'file name', |
| 8.2.3 | ʻemail' (data field) | email address of a spam message sender | The sender's e-mail address shall be submitted in the format in accordance with Specification RFC 5322 [18] | 'size': 'file size in bytes', 'base64': 'attachment in base64 format' |
| 8.3 | 'spamImage' (data block) | sample spam message | | }, 'fileLink': |
| 8.3.1 | 'sourceld' (data field) | identifier assigned by an information exchange participant | 128-bit identifier (GUID) generated in accordance with | 'http://domain.com/archive.rar' } }], |

| | | | Specification RFC 4122 [16] assigned by the Bank of Russia participant |
|-------|------------------------------|---|--|
| 8.3.2 | 'comment' (data field) | attachment description | textarea (text field) |
| 8.3.3 | 'dateTimeAt' (data field) | date and time when the file was added | data provision format in accordance with Specification RFC 3339 [11] |
| 8.3.4 | 'file' (data block) | data file containing additional materials | Specify the name and size of the file (no more than 5 MB) and perform Base64 encoding |
| 8.3.5 | 'fileLink' (data field) | link for obtaining (downloading) a data file containing additional materials | Specify the URL for downloading the file, if its size exceeds 5 MB, in accordance with Specification RFC 3986 [15] |

12.3.9. Computer attacks related to detecting the interaction of information infrastructure facilities of information exchange

participants with Botnet command centres [controlCenters] (for [INT] vector)

| Data block (field) No. | ldentifier of data block (field) | Data block (field) content | Data field format | E-mail format |
|---------------------------------|-------------------------------------|--|--|---|
| 9.2 | 'hostUrl' (data field) | URL hosting the Botnet Command Centre | URL in accordance with Specification RFC 3986 [15] | 'controlCenters': [{ 'hostUrl': 'http://example.com ', |
| 9.3 | 'intruderIp' (data field) | | Logical IPv4 address shall comply with Specification RFC 791 [12] | 'intruderIp': '1.1.1.1', 'intruderActions': 'what preceded the incident', |
| 9.4 | 'intruderActions' (data field) | description of unauthorised activity in the information infrastructure of an information exchange participant | textarea (text field) | 'description': 'additional description of the Botnet command centre', 'nodes': [{ 'ip': '127.0.0.1', 'lastRequestRateTime': '2018-03- 22T08:14:38Z ' |
| 9.5 | 'description' (data field) | additional description Botnet command centre | textarea (text field) | }] }], |
| 9.6 | 'nodes' (data block) | | If it is necessary to specify several data field values (ip, lastRequestRateTimeAt), specify one or several objects in the data block | |
| 9.6.1 | ʻip' | external IP address | Logical IPv4 address shall comply with | |

| | (data field) | (of an information exchange participant) | Specification RFC 791 [12] | | | | | | |
|-------|--------------|---|--------------------------------------|----|--|--|--|--|--|
| 9.6.2 | 'lastRequest | 0117 | data submission format in accordance | ce | | | | | |
| | RatetimeAt' | interaction with the | with Specification RFC 3339 [11] | | | | | | |
| | (data field) | Botnet command centre | | | | | | | |

12.3.10. Computer attacks related to a change (substitution) of the mobile subscriber identifier (IMSI) of the SIM card number, as well as the replacement of the mobile equipment identifier (IMEI) **[sim]** (for [EXT] vector)

| Data block (field) No. | ldentifier of data block (field) | Data block (field) content | Data field format | E | -mail format |
|---------------------------------|---|---|--|--------------------|---|
| 9.1 9.2 | 'mobileOperator' (data field) 'phoneNumber' | mobile telecom operator name mobile telephone | textarea (text field) In the KKKXXXNNNNNNN | telecom operator', | 'sim': { 'mobileOperator': 'name of mobile |
| | (data field) | number | format, where: KKK – a country code of one to three characters; XXX – operator's code; NNNNNNN - seven characters of the number. The telephone number shall be provided without a plus sign (+), | | <pre>'phoneNumber': '1212312345678', 'imsi': 'unique sim card number', 'imsiChangedAt': '2018-03- }, 22T08:08:49Z '</pre> |
| 9.3 | 'imsi' (data field) | unique SIM card number (imsi number) | spaces (_) and separation signs (-). | | |
| 9.4 | 'imsiChangedAt' (data field) | date and time when the IMSI change was recorded | data submission format in accordance with Specification RFC 3339 [11] | | |

12.3.11. Computer attacks related to the dissemination of information related to offers and/or provision of financial services in the Russian Federation by persons not entitled to provide them in accordance with the legislation of the Russian Federation. Posting prohibited content on the Internet **[prohibitedContents]**(for [EXT], [INT] vector)

| Data block (field) No. | ldentifier of data block (field) | Content of data block (field) | Data field format | E-mail format |
|---------------------------------|-------------------------------------|--|---|----------------------------------|
| 12.1 | ʻsources' (data block) | identifiers of prohibited content sources | If it is necessary to specify several values of data fields (ip, url), specify one or several objects in the data block 'target' | ʻprohibitedContents': [{ |
| 12.1.1 | 'ip' (data field) | IP address | Logical IPv4 address shall comply with Specification RFC 791 [12] | 'type': 'type of content' }], |
| 12.1.2 | ʻurl' (data field) | URL-address | URL in accordance with Specification RFC 3986 [15] | |
| 12.2 | 'type' (data field) | prohibited content type | textarea (text field) | |

12.3.12. Computer attacks related to information that misleads information exchange participants and their clients, as well as other persons interacting with them, about the ownership of the information disseminated via the Internet due to the similarity of domain names, design or content. Phishing **[phishingAttacks]** (for [EXT], [INT] vector)

| Data block (field) No. | Data block (field) identifier | Content of data block (field) | Data field format | E-mail format |
|---------------------------------|-------------------------------------|----------------------------------|---------------------------------------|---------------------------------------|
| 11.2 | 'harmful' | | If it is necessary to specify several | 'phishingAttacks': [{ |
| | (data block) | identifiers | values of data fields (ip, url), | 'harmful': [{ |
| | | | specify one or several objects in | ʻip': '127.0.0.1', |
| | | | the data block 'harmful' | 'url': 'http://example.com' |
| | | | | }], |
| 11.2.1 | 'ip' | IP address | Logical IPv4 address shall comply | 'fixationAt': '2018-03-22T08:14:38Z', |
| | (data field) | | with Specification RFC 791 [12] | 'messageAttachment': { |
| | | | | 'sourceld': 'f34030ef-358a-445c- |
| 11.2.2 | 'url' | URL-address | URL in accordance with Specification | 8567- |
| | (data field) | | RFC 3986 [15] | 25985ce6d91c', |
| | | | | 'comment': 'attachment description', |

| 11.3 | ʻfixationAt' (data field) | date and time of phishing message recording | data submission format in accordance with Specification RFC 3339 [11] | | 'dateTimeAt': '2018-03-22T08:14:38Z ', 'file': { |
|--------------|---|---|--|---|--|
| 11.4 | ʻmessage Attachment' (data block) | phishing message sample | | bytes', | 'name': 'file name', 'size': 'file size in |
| 11.4.1 | ʻsourceld' (data field) | identifier assigned by an information exchange participant | 128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by the information exchange participant | base64 format' 'http://domain.com/archive.rar' | 'base64': 'attachment in }, 'fileLink': |
| 11.4.2 | 'comment' (data field) | attachment description | textarea (text field) | }], | |
| 11.4.3 | 'dateTimeAt' (data field) | date and time when the file was added | data submission format in accordance with Specification RFC 3339 [11] | | |
| 11.4.4. 1 | 'file' (data block) | data file containing additional materials | Specify the name and size of the file (no more than 5 MB) and perform Base64 encoding | | |
| 11.4.5 | 'fileLink' (data field) | link for obtaining (downloading) a data file containing additional materials | Specify the URL for downloading the file, if its size exceeds 5 MB, in accordance with Specification RFC 3986 [15] | | |

12.3.13. Computer attacks related to the placement on the Internet of information enabling illegal access to information systems of information exchange participants and their customers used in the provision (receipt) of financial services, including through illegal access to confidential customer information. Posting a malicious resource on the Internet **[prohibitedContents]** (for [EXT], [INT] vector)

| Data block (field) No. | ldentifier of data block (field) | Data block (field) content | Data field format | E-mail format |
|---------------------------------|-------------------------------------|-------------------------------|---|-------------------------------------|
| 13.1 | 'sources' (data block) | | If it is necessary to specify several values of data fields (ip, url), specify one or several objects in the data block 'target' | <pre>'maliciousResources': [{</pre> |
| 13.1.1 | 'ip' (data field) | IP address | Logical IPv4 address shall comply with Specification RFC 791 [12] | |

12.3.14. Computer attacks related to a change in the content [changeContent] (for [INT] vector)

| Data block (field) No. | Identifier of data block (field) | Content of data block (field) | Data field format | E-mail format |
|---------------------------------|-------------------------------------|---|---|--|
| 14.1 | 'targets' (data block) | identifiers of attacked objects which content was changed | If it is necessary to specify several values of data fields (ip, url), specify one or several objects in the data block 'target' | 'changeContent': [{ |
| 14.1.1 | 'ip' (data field) | IP address | Logical IPv4 address shall comply with Specification RFC 791 [12] | <pre>'type': 'type of changed content' }],</pre> |
| 14.1.2 | ʻurl' (data field) | URL-address | URL in accordance with Specification RFC 3986 [15] | |
| 14.2 | 'type' (data field) | type of changed content | textarea (text field) | |

12.3.15. Computer attacks related to the scanning of software ports of information infrastructure facilities of information exchange participants by persons not authorised to do so **[scanPorts]** (for [INT] vector)

| Data block (field) No. | ldentifier of data block (field) | Content of data block (field) | Data field format | E-mail format |
|---------------------------------|-------------------------------------|----------------------------------|--|--|
| 15 | 'sourceld' | U 1 | 128-bit identifier (GUID) generated | 'scanPorts': [{ |
| | (data field) | information exchange | in accordance with Specification RFC | 'sources': [{ |
| | | participant | 4122 [16] assigned by the | 'ip': '127.0.0.1' |
| | | | information exchange participant | }], |
| | | | - · · · | 'ports': ['23'], |
| 15.2 | 'sources' | malicious activity source | If it is necessary to specify several | 'method': 'information on scanning methods |
| | (data block) | identifiers | values of the data field (ip), specify | or software used for this purpose', |
| | . , | | one or several objects in the data | 'startTimeAt': '2018-03- |
| | | | block 'sources' | 22T08:14:38Z', 'endTimeAt': '2018- |
| 15.2.1 | ʻip' | IP address | Logical IPv4 address shall comply with | 03-22T08:14:38Z' |
| | (data field) | | Specification RFC 791 | }], |

| | | | [12] |
|------|---------------|--------------------------|-------------------------------------|
| 15.3 | 'ports' | port numbers that have | textarea (text field) |
| | (data field) | been scanned | |
| 15.4 | 'method' | information on scanning | textarea (text field) |
| | (data field) | methods or software used | |
| | | for this purpose | |
| | | | |
| | | | |
| 15.5 | 'startTimeAt' | coop start time | data provision format in accordance |
| | (data field) | scan start time | with Specification RFC 3339 [11] |
| | | | |
| 15.6 | 'end time' | | data provision format in accordance |
| | (data field) | scan end time | with Specification RFC 3339 [11] |
| | | | |

12.3.16. Other computer attacks against information infrastructure facilities of information exchange participants and their clients **[other]** (for [INT], [EXT] vector)

| 16.1 | 'description' (data field) | description of a computer attacked object | textarea | 'other': { 'description': 'computer attack description', |
|--------|-------------------------------|---|--|---|
| 16.2 | (data filed) (data block) | identifiers of another source of malicious, prohibited content /resource | | 'target': { |
| 16.2.1 | 'ip' (data field) | IP address | Logical IPv4 address shall comply with Specification RFC 791 [12] | 'type': 'type of content', 'attachment': { 'sourceld': 'f34030ef-358a-445c- |
| 16.2.2 | ʻurl' (data field) | URL-address | URL in accordance with Specification RFC 3986 [15] | 8567- 25985ce6d91c', |
| 16.2.3 | 'type' (data field) | other type of prohibited, malicious, modified content | textarea (text field) | 'comment': 'comment to attachment', 'dateTimeAt': '2018-03- 22T08:14:38Z', |
| 16.3 | 'attachment' (data block) | additional data to identify a computer attack | | 'file': { 'name': 'file name', 'size': 'file size in |
| 16.3.1 | ʻsourceld' (data field) | identifier assigned by an information exchange participant | 128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by the information exchange participant | bytes', 'base64': 'attachment in base64 format' }, 'fileLink': |
| 16.3.2 | 'comment' | attachment description | textarea (text field) | 'http://domain.com/archive.rar' } } |

| | (data field) | | |
|--------|------------------------------|---------------------------------------|---|
| 16.3.3 | 'dateTimeAt' (data field) | date and time when the file was added | data submission format in accordance with Specification RFC 3339 [11] |
| 16.3.4 | 'file' (data | data file containing | Specify the name and size of the file |
| | block) | additional materials | (no more than 5 MB) and perform |
| | | | Base64 encoding |
| 16.3.5 | 'fileLink' | link for obtaining | Specify the URL for downloading the |
| | (data field) | (downloading) a data file | file, if its size exceeds 5 MB, in |
| | | containing | accordance with Specification RFC |
| | | additional materials | 3986 [15] |

12.4. Technical recommendations of the information bulletin **[signatures]**

| Data block (field) No. | ldentifier of data block (field) | Data block (field) content | Data field format | E-mail format |
|---------------------------------|-------------------------------------|---|--|---|
| 2.1 | 'mainActions' (data field) | recommended measures to counter computer attack | textarea (text field) | 'mainActions': 'recommended measures to counter computer attack', 'signatures': [{ 'identifier': 'signature identifier', 'yara': |
| 2.2 | ʻsignatures' (data block) | signature | If it is necessary to specify several data field values (identifier, yara, snort), specify one or several objects in the data block 'source' | 'yara-rule', 'snort': ['rule1','rule2'] }] } } |
| 2.3 | 'identifier' (data field) | unique signature identifier | sequence of symbols obtained as a result of calculating the MD5 hash function | |
| 2.4 | ʻyara' (data field) | YARA-rule | textarea (text field) | |
| 2.5 | ʻsnort' (data field) | Snort-rules | <pre>submission format in the form of: <action> <protocol> <ip addresses="" of<br="">senders> <senders' ports=""> <destination operator=""> <ip addresses of recepients> <recipient ports> (key_1: value_1; key_2: value_2; key_n: value_n;)</recipient </ip </destination></senders'></ip></protocol></action></pre> | |

13. The form of data submission used by information exchange participants to send information to the Bank of Russia on planned measures to disclose information on identified incidents related to violations of data protection requirements and timeframes for their submission to the Bank of Russia

13.1. Mandatory conditions and time characteristics of information provision

Mandatory information conditions:

[O] – data block (field) information shall be provided as required;

[N] – data block (field) information shall be provided if it is technically feasible. <u>Time characteristics of</u> information provision (stages of information provision):

[1] – data block (field) information shall be provided by an information exchange participant as part of the initial notification no later than one business day before the incident disclosure event;

[2] – data block (field) information shall be provided by an information exchange participant as part of the subsequent notification if information on possible incident disclosure is changed.

| 13.2. | Identification data on planned | measures to disclose information | about incidents. Data block [HEADER] |
|-------|--------------------------------|----------------------------------|--------------------------------------|
|-------|--------------------------------|----------------------------------|--------------------------------------|

| Data block (field) No. | ldentifier of data block (field) | Content of data block (field) | Data field format | E-mail format | Obligation of informing | Stages of information provision |
|---------------------------------|---------------------------------------|---|---|---|----------------------------|---------------------------------------|
| 1.1 | 'schemaType' (data field) | type of electronic message | Specify the value of [PUB] – publication | { | [0] | [1], [2] |
| 1.2 | , , , , , , , , , , , , , , , , , , , | electronic message type scheme version | textarea (text field) | 'pub', 'schemaVersion': '1', 'version': '1', | [0] | [1], [2] |
| 1.3 | 'version' | version number of an electronic | numeric value (int) | 'memberld':'9527dd0c-0765-4f1c-8f5f- 70a02cf4046c', 'sourceld':'f34030ef-358a-445c- 8567-25985ce6d91c', 'publishedAt': '2002-10- 02T15:00:00.05Z', | [0] | [1], [2] |

| | (data field) | message during information exchange | | ʻr }, | nodifiedAt': '2002-10-02T15:00 | :00.05Z' | | |
|-----|-------------------------------|---|---|----------|--------------------------------|----------|-----|----------|
| 1.4 | 'memberld' (data field) | exchange participant identifier | 128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by the Bank of Russia | | | | [0] | [1], [2] |
| 1.5 | ʻsourceld' (data field) | identifier assigned by an information exchange participant | 128-bit identifier (GUID) generated in accordance with Specification RFC 4122 [16] assigned by an information exchange participant | | | | [0] | [1], [2] |
| 1.6 | ʻpublishedAt' (data field) | | data provision format in accordance with Specification RFC 3339 [11] | | | | [0] | [1], [2] |
| 1.7 | ʻmodifiedAt' (data field) | | data provision format in accordance with Specification RFC 3339 [11] | | | | [0] | [2] |

13.3. Description of planned measures to disclose information about incidents. Data block **[PUB]**

| Data block (field No. | hleals (field) | Content of data block (field) | Data field format | E-mail format | Obligation of informing | Stages of information provision |
|--------------------------------|---------------------------|---|-----------------------|---------------|----------------------------|---------------------------------------|
| 2.1 | ʻorgName' (data field) | name of the organisation that is an information exchange participant | textarea (text field) | 'pub': { | [0] | [1], [2] |
| 2.2 | 'persons' | contact data | If it is necessary to | | [0] | [1], [2] |

| | (data block) | of the responsible person | indicate several values of data fields (lastName, middleName, firstName, landlineNumber, mobileNumber, email, position, eventScheduledAt) specifies one or several | <pre>'firstName': 'name',</pre> | | |
|-------|----------------------------------|--|---|--|-----|----------|
| | | | objects in the block of data 'persons' | 'subjectOfFederation': '00', 'locality': 'residential area name' | | |
| 2.2.1 | ʻlastName' (data field) | surname | textarea (text field) | }, 'description': 'additional data on the event', | [0] | [1], [2] |
| 2.2.2 | ʻmiddleName' (data field) | middle name | textarea (text field) | - 'typeOfActivity': ['type of planned event'], | [0] | [1], [2] |
| 2.2.3 | ʻfirstName' (data field) | name | textarea (text field) | 'nameOfActivity': name of the planned event or resource where information is to be disclosed', | [0] | [1], [2] |
| 2.2.4 | 'landlineNumber' (data field) | stationary telephone | textarea (text field) | 'text': 'text for the planned event', 'messageAttachment': { | [0] | [1], [2] |
| 2.2.5 | 'mobileNumber' (data field) | mobile telephone | textarea (text field) | 'sourceld': 'f34030ef-358a-445c- 8567- | [0] | [1], [2] |
| 2.2.6 | ʻemail' (data field) | e-mail addres | The sender's e-mail address shall be submitted in the format in accordance with Specification RFC 5322 [18] | attachment', 'dateTimeAt': '2018-03- 22T08:14:38Z ', 'file': { 'name': 'file name', | [0] | [1], [2] |
| 2.2.7 | ʻposition' (data field) | position | textarea (text field) | 'size': 'file size in bytes', 'base64': 'attachment in | [0] | [1], [2] |
| 2.3 | (data field) | date and time of the planned event (speech) or publication of information on incidents | data provision format in accordance with Specification RFC 3339 [11] | Base64 formate' }, 'fileLink': ' http://domain.com/archive.rar ' } } | [0] | [1], [2] |
| 2.4 | 'location' (data block) | event (speech) location | | | [0] | [1], [2] |

| 2.4.1 | ʻsubjectOfFedera- (data field) | upper-level OKTMO code | textarea (text field) |
|-------|--|---|---|
| 2.4.2 | 'locality' (data field) | name of a residential area | textarea (text field) |
| 2.5 | 'description' (data field) | additional data on the event | textarea (text field) |
| 2.6 | 'typeofActivity' (data field) | type of the planned event | One or more codes should to be selected from the limited set of possible values: • [CNF] – conference; • [PBE] – publication using an external resource (including printed publications); • [PBI] – publication on the information exchange participant's own resource (including |
| 2.7 | ʻnameofActivityʻ (data field) | name of the planned event or resource where information is to be disclosed | printed publications) textarea (text field) |
| 2.8 | 'text' (data field) | text to the planned event | textarea (text field) |
| 2.9 | 'messageAttachm e nt' (data block) | the information being disclosed | |
| 2.9.1 | ʻsourceld' (data field) | identifier assigned by an information exchanged participant | 128-bit identifier (GUID) generated in accordance with |

| | | | Specification RFC 4122 |
|-------|---------------------------|---------------------------|-----------------------------|
| | | | [16] assigned by an |
| | | | information exchange |
| | | | participant |
| 2.9.2 | 'comment' (data field) | attachment description | textarea (text field) |
| 2.9.3 | | date and time | data provision format in |
| | 'dateTimeAt' | when the file | accordance with |
| | (data field) | was added | Specification RFC 3339 [11] |
| 2.9.4 | 'file' | data file | Specify the name and size |
| 2.5.1 | (data block) | uutu me | of the file (no more than 5 |
| | (| | MB) and perform |
| | | | encoding in |
| | | | Base64 formate |
| 2.9.5 | 'fileLink' | | Specify the URL for |
| | (data field) | - | downloading the file, if |
| | | | its size exceeds 5 MB, in |
| | |) a data file | accordance with |
| | | containing additional | Specification RFC 3986 |
| | | materials | [15] |
| | | materials | |

14. Conditions for information exchange participants to submit to the Bank of Russia data on detected incidents related to violation of data protection requirements

14.1. Informing the Bank of Russia about revealed events of the type:

[MTR_WC] means the receipt by the money transfer operator serving the payer, including the electronic money operator, of notifications in the form stipulated by the agreement from customers which include individuals, legal entities, individual entrepreneurs or individuals engaged in private businesses about cases and (or) attempts to transfer funds without the customer's consent, including about the use of electronic payment instruments;

[A_SC] means the receipt by the payment system settlement centre notifications from payment system participants about debiting funds from their correspondent accounts without their consent and/or using distorted information contained in the instructions of payment clearing centres or payment system participants;

[UO_WC] means the identification by the money transfer operator serving the payer, including the electronic money operator, of transactions with signs of a money transfer without the customer's consent as established by the Bank of Russia and posted on the Bank of Russia website;

[FMA_WC] means the receipt of notifications from customers which include individuals, and (or) individual entrepreneurs, and (or) individuals engaged in private businesses in accordance with the procedure established by the legislation of the Russian Federation, and (or) legal entities about an illegal financial transaction;

[MTR_UA] means the identification by the money transfer operator serving the payer, including the electronic money operator, of money transfer operations and cash receipts as a result of unauthorised access to the information infrastructure of the money transfer operator, including when the balance of electronic funds is reduced, except for virtual payment cards;

[FMS_UA] means the identification of illegal financial transactions conducted as a result of unauthorised access to information infrastructure facilities of a non-bank financial institution;

[UPT_PSP] means an unauthorised withdrawal of funds of the money transfer operator at ATMs;

[DT_ALL] means a failure to provide services by the money transfer operator for more than two hours in total for all constituent territories of the Russian Federation where the money transfer operator transfers funds using payment cards, their details and (or) remote banking systems (funds);

202

[DT_SEL] means a failure to provide services by the money transfer operator for more than two hours in total for individual constituent territories of the Russian Federation where the money transfer operator transfers funds using payment cards, their details and (or) remote banking system (s);

[UPT_EMP] means an unauthorised withdrawal of funds of the electronic money operator at ATMs;

[DT_SC] means that a settlement centre has failed to provide settlement services for more than one operational day;

[DTPT_SC] means a failure by a settlement centre to make payments during an operational day against orders of a payment clearing centre or payment system participants accepted for execution;

[DT_CC] means the termination by a clearing centre in providing payment clearing services for a period of more than one operational day;

[DTPT_CC] means a clearing centre's failure to clear a payment subject to the accepted orders of payment system participants during one operational day;

[DT_OC] means the suspension by an operational centre of the provision of operational services for a period of more than two hours;

[DT_FS_ALL] means a financial institution's failure to provide services for more than two hours in total for all constituent territories of the Russian Federation where the financial institution provides financial services;

[DT_FS_ALL] means a financial institution's failure to provide services for more than two hours in total for individual constituent territories of the Russian Federation where the financial institution provides financial services;

shall be carried out for each event separately.

14.2. Identification by an information exchange participant of computer attacks which may lead to the events specified in Clause 14.1:

[PSP_CMTR] means the detection by the money transfer operator, including the electronic money operator, and/or the payment infrastructure service provider of attacks the consequences of which may lead to events and attempts of making money transfers without their customer's consent;

[CO_CFS] means the detection by a credit institution of computer attacks, the consequences of which may lead to events and attempts to carry out a financial (banking) transaction without its customer's consent;

[NCFI_CFS] means the detection by a non-bank financial institution of computer attacks, the consequences of which may lead to events and attempts to carry out a financial (banking) transaction in the financial market without its customer's consent;

To be done according to the following criteria (V is the information provision criterion):

| | | | | | | | • | Types of | comput | er attac | ks | | | | | |
|---|-------------------|------------------------------------|--------------------------------|-------------|---|-----------------------------------|----------------|---|-------------------|---|--------------------------|---|---------------------------|----------------------------|--------------------|---------|
| Objects of computer attacks | | | | xternal | of a computer attack on the I perimeter of the information | | | detection of a computer attack on the internal perimeter of the information infrastructure | | computer attack against customers or employees of an information exchange participant | | detection of a computer attack against payment infrastru cture elements | other types of attacks | | | |
| System levels | [ddos Attacks] | [traffic Hijack Attack s] | [vulne r abili- ties] | [spams] | [phishing Attacks] | [mali- cious Resour ces] | [mal- ware] | [control Centers] | [brute Forces] | [scan- Ports] | [socialEn gineering | [sim] | [atm Attacks] | [prohibi ed Content] | [change Content | |
| [hw] – hardware | v | | v | | | | v | | v | v | | v | v | | | v |
| [net] - network equipment | v | v | v | | | v | v | V | V | v | | | | | | v |
| [net_s] – network applications and services | v | | v | | | | v | | | | | | | | | v |
| [hw_s] – virtualisation server components, software infrastructure | v | v | v | | | | v | v | | | | | | | | v |
| [os] – operating systems, database management systems, application servers | v | | v | | | | v | v | | | | | | | | v |
| The level of AS and applications operated for the provision of | [ddos Attacks] | [traffic Hijack At- | [vulne r abili- | [spams] | [phishing Attacks] | [malicio us Re- | [mal- ware] | [control Centers] | [brute Forces] | [scan Ports] | [social Enginee r- | [sim] | [atm Attacks] | [prohi- bited | [change Content | [other] |

| services within business or technological processes of an information exchange participant | | tacks] | ties] | | sources] | | | | | ing] | | Content s] | |
|--|---|--------|-------|---|----------|---|---|---|---|------|---|---------------|---|
| [rbs] — a remote banking system | v | | v | | | v | | v | v | | | | v |
| [front-office] – a payment card transaction processing system | v | | v | | | v | | v | v | | v | | v |
| [web] – Internet information resources | v | | | | | v | | v | v | | | | v |
| [abs] – an automated banking system | V | | v | | | v | | v | v | | | | v |
| [back-office] – a system for post- transaction servicing of payment card transactions | v | | v | | | v | | v | v | | | | v |
| [int-services] – internal information infrastructure for supporting the business processes of an information exchange participant (mail servers, file servers) | | | v | V | v | v | V | V | v | | | | v |

| [participant_w] means terminal equipment (automated workstation) used by employees of an information exchange participant | | | v | v | | | | | | | v | v | | v | v | v |
|---|-------------------|-------------------------------------|---------------------------------|-------------|---------------------------------|--|----------------|----------------------|-------------------|-----------------|-----------------------------|-------|------------------|-----------------------------------|---------------------|-------------|
| The level of AS and applications operated by an information exchange participant's client | [ddos Attacks] | [traffic Hijack At- tacks] | [vulne - rabili- ties] | [spams] | [phish- sing Attacks] | [mali- cious Resour ces] | [mal- ware] | [control Centers] | [brute Forces] | [scan Ports] | [social Enginee ring] | [sim] | [atm Attacks] | [prohi- bited Content s] | [change Content] | |
| [cfs] – a file server | | v | v | | | | v | | | | | | | | | v |
| [crbs] — a remote banking system | v | v | v | | | | v | | | | | | | | | v |
| [ecs] – an e-mail account | | | | | v | v | v | | | | | | | | | v |
| [client_w] — an automated systems used by employees of an information exchange participant's client | | | v | | | | | | | | v | v | | v | v | v |
| Other system | [ddos Attacks] | С | [vulne r- abili- ties] | [spam s] | [phishi ng Attack s] | [mali- ciousR e- source s] | [mal- ware] | [contro Centers | [brute Forces | - | [social Engine ering] | [sim] | [atm Attacks | [prohib ited Conten ts] | [chang Conten | [other] |
| [oth] – other system | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V |

14.3. Assessment of the severity of consequences of an incident. When informing the Bank of Russia about identified incidents related to a violation of information protection requirements by an information exchange participant, it is necessary to make a relative (qualitative) assessment of the scale (severity of consequences) of the occurrence of data protection events in accordance with the following criteria:

| | | Characteristics of the scale of | Т | hreshold values | |
|----|--|---|-------------------|--------------------|--------------------|
| N⁰ | Code and type of the event | consequences of the occurrence of the event as a whole | Moderate [MOD] | Essential [ESS] | Critical [CRIT] |
| | | The amount of debited (withdrawn) funds, rubles | 1,400,000 | 5,000,000 | 15,000,000 |
| 1 | [UPT_PSP] – unauthorised withdrawal of funds of the money transfer operator at ATMs | The number of unauthorised access events, units | 100 | 500 | 1,000 |
| | | The amount of operational expenses of the money transfer operator as a result of debits (withdrawals) of funds, rubles | 2,000,000 | 10,000,000 | 25,000,000 |
| 2 | [DT_ALL] – a failure by the money transfer operator to provide services for a period of more than two hours in total to individual constituent territories of the Russian Federation where the money transfer operator transfers funds using payment cards, their details and (or) a remote banking system (s); [DT_SEL] – a failure by the money transfer operator to provide services | The number of events related to non-provision of money transfer services, unit | - | - | 1 |
| | for a period of more than two hours in total to individual constituent territories of the Russian Federation where the money transfer operator transfers funds using payment cards, their details and (or) a remote banking system (s); | A region of non-provision of money transfer services, constituent territories of the Russian Federation | 2 | 5 | 10 |
| | | The amount of a decrease in the electronic money balance, rubles | 100,000 | 500,000 | 1,000,000 |
| 3 | [UPT_EMP] – unauthorised withdrawal of funds of the e-money operator at ATMs | The number of unauthorised access events, units | 100 | 500 | 1,000 |
| | | The amount of operating expenses of the electronic money operator as a result of the decrease in the electronic money balance, rubles | 500,000 | 1,500,000 | 5,000,000 |

| 4 | [DT_SC] means that a settlement centre has failed to provide settlement services for more than one operational day; [DTPT_SC] means a settlement centre's failure to conduct payment transactions during an operational day as per accepted orders of a payment clearing centre or payment system participants | The number of events related to the non-provision of settlement services, units | 3 | 5 | 10 |
|---|---|--|---|---|----|
| 5 | [DT_CC] means the termination by a clearing centre in providing payment clearing services for a period of more than one operational day; [DTPT_CC] means a settlement centre's failure to clear payments during an operational day according to accepted orders of payment system participants | The number of events related to non-provision of payment clearing services, units | 3 | 5 | 10 |
| 6 | [DT_OC] means the suspension by an operational centre of the provision of operational services for a period of more than two hours | The number of events related to non-provision of operational Services, units | 3 | 5 | 10 |
| 7 | [DT_FS_ALL] means a non-bank financial institution's failure to provide services for more than two hours in total to all constituent territories of the Russian Federation where this non-bank financial institution provides financial services; [DT_FS_ALL] means a non-bank financial institution's failure to provide services for more than two hours in total to individual constituent territories of the Russian Federation where this non-bank financial institution provides services for more than two hours in total to individual constituent territories of the Russian Federation where this non-bank financial institution provides financial services | The number of events related to non-provision or untimely provision of financial services, units A region of non-provision of money transfer services, units | 3 | 5 | 10 |

STO BR BFBO-1.5-2018

15. Description of the technology for preparing and sending electronic messages during information exchange with the Bank of Russia

15.1. Electronic message preparation technology¹

15.1.1. An electronic message shall be prepared using:

- personal account of the participant (https://lk.fincert.cbr.ru);
- a specialised application installed by an information exchange participant (hereinafter,

the desktop application);²

15.1.2. The personal account of an information exchange participant makes it possible to generate an electronic message by filling in the on-line form for sending data in accordance with the provisions of this standard.

15.1.3. The desktop application makes it possible to generate an electronic message by filling in the application form for sending data to the FINCERT ASIP (Automated System of Incident Processing)

15.2. Electronic messaging technology³

Information is transmitted via the Bank of Russia's information resources on the Internet by providing information exchange participants with access to their personal accounts (https://lk.fincert.cbr.ru).

Backup methods of information transmission to the Bank of Russia are used by an information exchange participant only in cases when the personal account of the information exchange participant does not have telecommunication accessibility and (or) it is not technically feasible to transmit information. Backup methods of information transmission include:

- use of e-mail (fincert@cbr.ru);
- telephone calls to the Bank of Russia (+ 7 (495) 772 70 90).⁴

¹ The protection of the transmitted information is implemented using the certified CIPF established in accordance with document BCMD.42 5790.520.13.2 'Participant's Manual for Working with FinCERT ASIP' (using the certified CIPF 'Continent-TLS'), The participant who sends information to FinCERT shall be identified and authenticated on the basis of information transmitted to FinCERT (information about the participant).

² It is transferred to FinCERT as part of the participant's package when the exchange participant is connected to the ASIP (when updating the application, its versions are posted on the FinCERT specialised ASIP portal – https://portal.fincert. Cbr.ru in the section 'FinCERT ASIP (Participant Documentation and Software)'). Access to the FinCERT ASIP specialised portal without the installation of a certified CIPF is not provided.

³ The protection of the transmitted information is implemented using the certified CIPF established in accordance with document BCMD.42 5790.520.13.2 'Participant's Manual for Working with FinCERT ASIP' (using the certified CIPF 'Continent-TLS'), The participant who sends information to FinCERT shall be identified and authenticated on the basis of information transmitted to FinCERT (information about the participant).

⁴ Voice data are not protected. The caller is identified by interviewing him/her regarding the name of his/her organisation, full name, position and contact telephone number, which are compared with the participant's card.

15.2.1. When transmitting information via e-mail, it is necessary to indicate the subject matter of the message and the accompanying text with attaching the following files:

- the electronic message generated in accordance with Section 15.1 hereof;
- other files, the maximum size of which should not exceed 25 MB (if the specified size is exceeded, it is allowed to send files in several parts with archiving them in several emails).

15.2.2. When transmitting information using the personal account of an information exchange participant, fields marked 'required to be filled' with the possibility of adding attachments of up to 2 GB shall be filled in;

15.2.3. If samples of malicious software (viruses) are sent to the Bank of Russia for investigation, they shall be transmitted to the archive (rar or zip) with one of the following passwords: 'virus' or 'infected'. If the password is not set in the transferred archive, it is deleted automatically.

| Data submission form used by information exchange participants for registration with the Bank of Russia | Form of data submission used by information exchange participants to inform the Bank of Russia about incidents related to violation of data protection requirements and deadlines for their submission to the Bank of Russia | Form of data submission used by information exchange participants to send information to the Bank of Russia on planned measures to disclose information on identified incidents related to violation of data protection requirements and timeframes for their submission to the Bank of Russia | by information exchange | Data submission form used by information exchange participants to submit a request to the Bank of Russia on the establishment of a restriction on their bank (correspondent) accounts (sub- accounts) in the form of a ban on the debiting of funds in case of revealed incidents related to violation of data protection requirements |
|---|--|--|--|--|
| { | { | { | { | { |
| 'member- Id': '9527dd0c-0765-4f1c- 8f5f-70a02cf4046c', 'sourceld': 'f34030ef-358a-445c- 8567- 25985ce6d91c', 'pub- lishedAt': '2002-10- 02T15:00:00.05Z', 'modi- fiedAt': '2002-10- | 'sourceld': 'f34030ef- 358a-445c-8567- 25985ce6d91c', 'publishedAt': '2002- 10-02T15:00:00.05Z', 'modifiedAt': '2002- 10-02T15:00:00.05Z' }, 'incident': { 'fincertId': '20180324215113', | 'sourceld': 'f34030ef-358a-445c- 8567- 25985ce6d91c', 'publishedAt ': '2002-10- 02T15:00:00.05Z', 'modifiedAt ': '2002-10- 02T15:00:00.05Z' }, 'pub': { | <pre>'sourceld': 'f34030ef-358a-445c- 8567- 25985ce6d91c',</pre> | 8567- 25985ce6d91c', 'publishedAt ': '2002-10- 02T15:00:00.05Z' }, 'lockRequest': [{ 'sourceld': |

Annex 1. Schemes of interaction between an information exchange participant and the Bank of Russia

| 02T15:00:00.05Z' | 'fixationAt': '2002-10- | 'orgFullName': | 25985ce6d91c', | 'regNumber': |
|---|---|---------------------------------|---|--|
| }, | 02T15:00:00.05Z', | 'full name of the information | 'victim': | '123456789', |
| 'participant': { | 'description': | exchange participant', | 'information on the legal | 'uniqldentifier': |
| 'orgld': | 'incident description', | 'persons': [{ | status of the payer', | ʻ1234567891', |
| 'identifier of the type of | 'lawEnforcementRe- | 'last- | 'recipient': | 'actionStatus': 'status of the restriction on funds |
| the information exchange | quest': { | Name': 'last name', | 'information on the legal | debiting', |
| participant', | 'addressed': | ʻmid- | status of the recepient of | debiting, |
| 'orgBrand' | 'a subject who has applied to law | dleName': 'patronymic name', | funds', | 'dateTimeAt': '2018- |
| : 'brand name of the | enforcement agencies', | 'first- | 'payeeldenti- | 03- 22T08:14:38Z', |
| information exchange | 'request': | Name': 'name', | fier': { | 'text': |
| participant', | 'information on the fact of an | 'land- | | 'addition |
| | information exchange participant's | lineNumber': 'stationary | 'hash': | al description', |
| 'orgShortName': | appeal to the police', | telephone', | ⁽ P79969612A71BAB224C7CB | 'persons': { |
| 'short name of the | 'number': | 'mo- | 534FD7A0D3C1C78AD40664C | 'lastName': 'last name', |
| information exchange | 'application number from the | bileNumber': 'mobile | 48F12A9AE48FA441E11', | first- |
| participant', | register of crime reports', | telephone,' | | Name': 'name', |
| | 'numberTick | 'email' | 'hashSnils': 'B49087832A71BAB224C7CB | 'middle- |
| 'orgFullName': | - et': 'the ticket | : 'e-mail | 534FD7A0D3C1C78AD40664C | Name': 'patronymic name', |
| 'full name of the information exchange | number for accepting and | address', | 48F12A9AE48FA441E44' | 'land- |
| participant', | registering the application', | | }, | lineNumber': '1212312345678', |
| • • • | 'dateTimeAt | 'position': 'position' | | 'mo- |
| ʻorgE- mails': [ʻɑwer- | ': 'date and time of | }], | 'payer': { | bileNumber': '1212312345678', |
| mails': ['qwer- ty1@example.ru', | the application acceptance' | 'eventSched- | ʻbik': | 'email': |
| 'qwer | }, | uledAt': '2002- | '123456789', | 'qwerty1@example.ru', 'position': |
| - ty2@example.ru'], | 'assistance': | 10- 02T15:00:00.05Z', | 'inn': | 'position' |
| 'orgIncom- | 'identifier of the need to support the | 'location': { | '123456789000', | }, |
| ingEmail': 'requestsFrom- | information exchange participant by the Bank of Russia', | 'subjec- | ʻpay- | ťattachment': { |
| fincert@example.ru', | | tOfFederation': '00', | erName': 'organisation | 'sourceld' |
| ʻorgBik': | <pre>'vectorCode': 'computer attack vector identifier',</pre> | | name that is the payer', | : 'f34030ef-358a-445c-8567- |
| '123456789', | • | 'locality': 'residential | 'pay- | 25985ce6d91c', |
| 'or- | 'serviceType': [{ | area name' | erTransferId': { | 'comment': |
| gLegalEntityForm': '12345', | 'sourceld' | }, | (tree = = = = = = = = = = = = = = = = = = | 'attachment description', |
| 'orgBin' | : 'f34030ef-358a-445c-8567- 25985av6d91c', | 'description': | 'transferType': 'money transfer method | 'dateTimeAt': '2018- |
| : ['123456', | | 'additional data on the event', | type', | 03- 22T08:14:38Z', |
| '123456'], | 'type': 'type of the object under attack' | | -/// | ʻfile': { |
| 'orgInn': | or the object under attack | | | |
| '1234567890', | | | | |

| 'orgKpp': | 'name': | 'typeOfActivity | 'paymentCard': { | 'name': 'file name', |
|---------------------------|--|---|----------------------------|--------------------------|
| '123456789', | 'name of software/hardware', | ': ['type of the planned | | |
| 'orgOgrn': | 'version': | activity'], | 'number': | ʻsize': 'file size in в |
| ʻ1234567890000', | 'software/hardware version', | | '12341234123412', | bytes', |
| 'isp': [{ | 'description' | 'nameOfActivity': 'name | | 'base64': 'attachment in |
| | : 'additional description of the | of the planned activity or | 'sum': | |
| 'name': 'telecom | type of the attacked object' | resource where information is | 'amount of the money | base64 format' |
| operator name', | }], | to be disclosed', | transfer transaction using | } |
| operator name) | | 'text': 'text to | payment cards', | }] |
| 'ipAddress': | 'registration': { | the planned activity', | | } |
| ['192.168.1.0', | 'department | 'mes- | 'currency': | 1 |
| (192.168.2.0'] | ': 'the structural | sageAttachment': { | 'currency of the money | |
| | (organisational) unit of an | - | transfer transaction', | |
| }], | information exchange participant | 'sourceld': | | |
| 'software': | where the incident was registered | 'f34030ef | 'dateTimeAt | |
| [{ | (detected)', | - 358a-445c-8567- | ': '2018-01-13T09:14:38Z', | |
| | 'tech- | 25985ce6d91c', | , | |
| 'sourceId': | nicalDevice': 'incident registration | 'com | 'rrn': 'the | |
| 'f34030ef-358a-445c-8567- | technical device' | - ment': | number generated for a | |
| 25985ce6d91c', | }, | 'attachment description', | money transfer transaction | |
| | 'typeOfAttack': | attaciment acscription, | during its authorisation' | |
| 'type': 'type of | 'co | 'dateTimeAt': '2018-03- | | |
| software/hardware | mputer attack type code', | 22T08:14:38Z ', | ı | |
| of the information | 'measuresAn | ' | }, | |
| exchange participant', | dRecomendations': [{ | ʻfile': | 6 | |
| - | 'sourceld' | | 'settlement': { | |
| | : 'f34030ef-358a-445c-8567- | { 'name': 'file name', | | |
| 'name': 'name of | 25985ce6d91c', | | 'number': | |
| software/ | | 'size': 'file size in | '12345123451234512345', | |
| hardware', | 'dateTimeAt ': '2018-03-22T08:14:38Z ', | bytes', | | |
| | | | 'sum': | |
| | 'action': | 'base64': 'attachment in | 'amount of the money | |
| 'version': 'version of | 'actions taken to eliminate the | base64 format' | transfer transaction', | |
| software | incident' | }, | | |
| hardware used', | 'text': 'text of | ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, | 'currency': | |
| - | measures or recommendations' | ʻfileLink': ʻ | | |
| | 'attachment': | http://domain.com/archive.rar | | |
| | | , , , , , , , , , , , , , , , , , , , | | |
| | | , | | |
| | | } | | |

| | (| 1 | | |
|-------------------------|--------------------------------|---|-----------------------------|--|
| 'description': | { | } | 'currency of money transfer | |
| addition | | } | transaction', | |
| al description of | 'sourceld': 'f34030ef- | | | |
| software/hardware', | 358a- 445c-8567-25985ce6d91c', | | 'dateTimeAt | |
| }], | | | ': '2018-01-13T09:14:38Z' | |
| 'persons': | 'comment': | | | |
| [{ | 'attachm | | }, | |
| | ent description', | | | |
| 'memberId': | · · · | | 'phoneNumber': { | |
| '9527dd0c-0765-4f1c- | 'dateTimeAt': '2018- | | phonertamber . (| |
| 8f5f- 70a02cf4046c', | 03- 22T08:14:38Z', | | · · · · · | |
| 0151 /00020140400 ; | | | 'number': | |
| <i>,</i> | 'file': | | ʻ1212312345678', | |
| 'sourceld': | { | | | |
| 'f34030ef-358a-445c- | | | 'sum': | |
| 8567-25985ce6d91c', | 'name': 'file name', | | 'amount | |
| | | | of the transaction', | |
| 'lastName': 'last | 'size': 'file size in | | | |
| name', | bytes', | | 'currency' | |
| | • • | | : 'transaction | |
| 'middleName | 'base64': 'attachment in | | currency', | |
| ': 'patronymic name', | base64 format' | | | |
| | | | 'dateTimeAt | |
| 'firstName': | }, | | ': '2018-01-13T09:14:38Z' | |
| institutie : | | | . 2010 01 13103.14.002 | |
| Increal | 'fileLink': | | , | |
| 'name', | 'http://domain.com/archive.rar | | }, | |
| | 1 | | | |
| 'landlineNumber': | } | | 'idNumber': { | |
| 'stationary telephone', | }], | | | |
| | | | 'number': | |
| 'mobileNumber': ' | 'location': { | | ʻ1KoX6AA5VTdbBTkw27YEqK | |
| mobile telephone', | 'subjec- | | FaTtEQq97AAT', | |
| | tOfFederation': '00', | | | |
| 'email': 'e- | 'locality': | | 'sum': | |
| mail address', | 'residential area name' | | 'amount | |
| | }, | | of the transaction', | |
| (position) | | | | |
| 'position': | 'classification': { | | (aumona) | |
| 'positio | 'typeOfInci- | | 'currency' | |
| n', | | | : 'transaction | |
| - | | | currency', | |

| | dent': 'incident type', | 'dateTimeAt |
|----------------------------|--------------------------------------|----------------------------------|
| 'active': 'exitence of | 'ext': [{ | ': '2018-01-13T09:14:38Z' |
| access to the personal | | |
| account | | } |
| of an information exchange | 'events': 'data protection | |
| participant', | events', | }, |
| | | ʻde- |
| 'category': 'category of | 'method': 'the method of | vice': { |
| structural unitn | preparing and transferring | |
| of the responsible | transaction instructions which make | 'ip': 'network |
| person of an information | it possible to conduct a financial | address of the device', |
| exchange participant' | operation' | |
| }], | }], | 'imsi': 'international |
| ʻid_cii': | 'int': [{ | mobile subscriber identifier |
| 'identifier of the | | (individual subscriber |
| CII object', | 'events': 'data protection | number)', |
| 'orgType': | events', | |
| 'type of an information | , | 'imei': 'international |
| exchange participant', | 'typeOfIntruder': 'violator | mobile equipment |
| 'legalAd- | type' | identifier', |
| - | | |
| dress': { | }], | 'aiic': 'Acquiring insti- |
| <i>.</i> | 'damage': { | tution identification code (32 |
| 'oktmo': | ʻop- | поле ISO 8583)', |
| '12345678', | erating': 'assessment of | |
| | operational expenses of an | 'cati': 'Card acceptor |
| 'postalCode': 'postal | information exchange participant at | terminal identification (41 |
| code', | the moment of providing data on | field ISO 8583)', |
| | the occurrence of an incident (INT | |
| 'country': 'three- | vector)', | 'caic': 'Card acceptor |
| letter country code', | ʻrela- | identification code (42 поле |
| | tive': 'relative (qualitative) | ISO 8583)' |
| 'federalDistrict': | assessment of the scale (severity of | |
| 'federal district code', | consequences) of the incident | } |
| | implementation (INT vector)' | }, |
| | }, | 'payee': { |
| 'subjectOfFedera- | 'schemaCon | ʻbik': |
| tion': '00', | clusion': 'description of the money | ʻ123456789', |
| | withdrawal scheme', | |

| (6: | (··· · · | (*) | |
|---------------------------------------|-------------------------------------|------------------------------|--|
| · · · · · · · · · · · · · · · · · · · | 'attach- | 'inn': | |
| asld': 'e6668cfd- | ments': [{ | '123456789000', | |
| ae08- 4b02-a385- | | ʻpay- | |
| 88179dfb1097', | 'sourceld': 'f34030ef- | eeName': 'the name of | |
| | 358a- 445c-8567-25985ce6d91c', | the organisation that is the | |
| 'district': 'district', | , | payee', | |
| | (| | |
| | 'comment': | ʻpay- | |
| 'city': 'city', | 'attachm | eeTransferId': { | |
| | ent description', | | |
| 'cityDistrict': 'inner | | 'transferType': | |
| city district ['] , | 'dateTimeAt': '2018- | 'money transfer method | |
| | 03- 22T08:14:38Z', | type', | |
| | | type, | |
| 'locality': | 'file': | | |
| 'residential area,' | { | 'paymentCard': { | |
| | | | |
| 'street': 'street', | 'name': 'file name', | 'number': | |
| street i street, | , | '123412341234123412', | |
| | | 123412341234123412, | |
| 'house': 'house | 'size': 'file size in | | |
| number', | bytes', | 'sum': | |
| | | 'amount of the money | |
| 'building': | 'base64': 'attachment in | transfer transaction using | |
| 'bloc | base64 format' | payment cards', | |
| k/building', | | | |
| ky building , | }, | 'currency': | |
| <i>.</i> . | | 'currency of the money | |
| 'room': | 'fileLink': | transfer transaction using | |
| 'room/ | 'http://domain.com/archive.rar' | | |
| office', | | payment cards', | |
| | }] | | |
| 'additionalInforma | }, | 'status1': { | |
| ti on': 'additional | 'antifraud': [{ | | |
| information' | 'sourceld' | ʻen- | |
| | | rollment': 'transaction | |
| }, | : 'f34030ef-358a-445c-8567- | suspension identifier', | |
| | 25985ce6d91c', | suspension identifier, | |
| 'postAddress': | 'victim': | | |
| | 'information on the legal status of | | |
| [(aktma) | the payer', | | |
| { 'oktmo': | 'payerIdenti- | | |
| '12345678', | payeridenti- | | |
| | | | |
| 'postalCode': | | | |
| , ípostal | | | |
| P | | | |
| code', | fier': { | 'dateTimeAt': '2002- |
|--------------------------|------------------------------------|-------------------------|
| | | 10-02T15:00:00.05Z' |
| / | | 10 02113.00.002 |
| 'country': 'three- | 'hash': | |
| letter country code', | 'E25059612A71BAB224C7CB534FD7A | |
| | 0D3C1C78AD40664C48F12A9AE48FA | |
| 'federalDistrict': | 441E44', | }, |
| 'federal district code', | | |
| | 'hashSnils': | (asthlement) (|
| | 'C49337884A71BAB224C7CB438FD7 | 'settlement': { |
| 'subjectOfFe | A0D3C1C78AD40664C48F12A9AE48F | |
| dera- tion': '00', | A441E44' | 'number': |
| 'fi- | | ʻ123451234512345', |
| asld': '8abe47a7- | }, | |
| 24dd- 4951-ae16- | 'payer': { | 'sum': |
| f2781eba9d93', | ʻbik': | 'amount of the money |
| | | |
| (district), (district) | '123456789', | transfer transaction', |
| 'district': 'district', | 'inn': | |
| | ʻ123456789000', | 'currency': |
| 'city': 'city', | ʻpay- | 'currency of the money |
| | erName': 'name of the organisation | transfer transaction', |
| 'cityDistrict': 'inner | | |
| city district', | | 'status1': { |
| city district, | 'рау- | 566651.[|
| | erTransferId': { | |
| 'locality': | | 'en- |
| 'residential area,' | 'transferType': 'money | rollment': 'transaction |
| | transfer method type', | suspension identifier', |
| 'street': 'street', | | |
| , | 'paymentCard': { | |
| 'house': 'house | | 'dateTimeAt': '2002- |
| | | 10-02T15:00:00.05Z' |
| number' | 'number': | |
| | '123412341234123412', | |
| 'building': | | } |
| 'bloc | 'sum': 'amount of | |
| k/building', | the money transfer transaction | }, |
| | using payment cards', | |
| 'room': | | |
| 'room/ | | |
| office', | | |
| onice, | | |

| 'additionalInforma | | 'phoneNumber': { |
|--------------------------|--|-----------------------------|
| ti on': 'additional | 'currency': 'currency | |
| information' | of the money transfer transaction', | 'number': |
| | , , | |
| }, | | ʻ1212312345678', |
| | 'dateTimeAt': '2018- | |
| 'physicalAddress': | 01-13T09:14:38Z', | 'sum': |
| [{ | | 'amount |
| | 'rrn': 'the number | of the transaction', |
| <i>.</i> | generated for a money transfer | of the transaction, |
| 'oktmo': | | |
| '12345678', | transaction during its authorisation' | 'currency' |
| | | : 'transaction |
| 'postalCode': | }, | currency', |
| 'postal code', | | |
| postal coue, | 'settlement': { | (-1-1·-A) (|
| | settlement : { | 'status1': { |
| 'country': 'three- | | |
| letter country code', | 'number': | 'en- |
| | '12345123451234512345', | rollment': 'transaction |
| 'federalDistrict': | | suspension identifier', |
| | | |
| 'federal district code', | 'sum': 'amount of | |
| | the money transfer transaction', | |
| 'subjectOfFe | | 'dateTimeAt': '2002- |
| dera- tion': '00', | 'currency': 'currency | 10-02T15:00:00.05Z' |
| ʻfi- | of money transfers', | |
| | | } |
| asld': '8661e93f- | | J J |
| 6c6a- 4b19-b485- | 'dateTimeAt': '2018- | |
| 14e27e564169', | 01-13T09:14:38Z' | }, |
| | | |
| 'district': 'district', | | 'idNumber': { |
| | }, | |
| | ,, | |
| 'city': 'city', | | 'number': |
| | 'phoneNumber': { | '1KoX6AA5VTdbBTkw27YEqK |
| 'cityDistrict': 'inner | | FaTtEQq97AAT', |
| city district', | | |
| ,, | | 'sum': |
| | | 'amount of the transaction |
| 'locality': | | |
| 'residential area,' | | for changing the balance of |
| | | funds', |
| | | |
| | | 'currency': |
| | l de la construcción de la constru | |

| | 'number': | 'amount of the transaction | |
|---------------------|--------------------------------|-----------------------------|--|
| | | | |
| 'street': 'street', | '1212312345678', | for changing the balance of | |
| | | funds', | |
| 'house': 'house | 'sum': 'amount of | | |
| number', | the transaction', | 'status1': { | |
| | | | |
| <i></i> | <i>,</i> | | |
| 'building': | 'currency': 'currency | ʻen- | |
| 'block/building', | of the transaction', | rollment': 'transaction | |
| | | suspension identifier', | |
| 'room': | 'dateTimeAt': '2018- | | |
| 'room/office', | 01-13T09:14:38Z' | | |
| roomyonice , | 01 10100.14.002 | 'dateTimeAt': '2002- | |
| | | 10-02T15:00:00.05Z' | |
| 'additionalInforma | }, | 10-02115.00.00.052 | |
| ti on': 'additional | | | |
| information' | ʻidNumber': { | } | |
| }] | | | |
| | | ۱ | |
| } | 'number': | ſ | |
| } | '1KoX6AA5VTdbBTkw27YEqKFaTtEQq | } | |
| | 97AAT', | } | |
| | | , | |
| | 'sum': 'transaction | }] | |
| | amount', | } | |
| | aniount , | | |
| | - | | |
| | | | |
| | 'currency': 'currency | | |
| | of the transaction', | | |
| | | | |
| | 'dateTimeAt': '2018- | | |
| | | | |
| | 01-13T09:14:38Z' | | |
| | | | |
| | } | | |
| | J | | |
| | }, | | |
| | 'device': { | | |
| | | | |
| | 'ip': 'network address of the | | |
| | device', | | |
| | device, | | |

| 'imsi': 'international mobile subscriber identifier (individual subscriber number)', | | |
|---|--|--|
| 'imei': 'international mobile equipment identifier', | | |
| 'aiic': 'Acquiring institution identification code (32 field ISO 8583)', | | |
| 'cati': 'Card acceptor terminal identification (41 field ISO 8583)', | | |
| 'caic': 'Card acceptor identifi- cation code (42 поле ISO 8583)' } | | |
| }, 'payee': { 'bik': '123456789', | | |
| ʻinn': ʻ123456789000', ʻpay- | | |
| eeName': 'name of the organisation that is the payee', 'pay- | | |
| eeTransferId': { | | |
| funds', | | |



| cross-border banking', | | |
|--|--|--|
| ʻad- | | |
| ditionalTransactionApprove': [| | |
| | | |
| 'identifier of the additional | | |
| approval of the transaction' | | |
| 1 | | |
| } | | |
| • | | |
| }], | | |
| 'impacts': { | | |
| 'trafficHi- | | |
| jackAttacks': [{ | | |
| | | |
| 'sourceld': 'f34030ef- | | |
| 358a- 445c-8567-25985ce6d91c', | | |
| ʻle- | | |
| galAsPath': 'legal AS-Path', | | |
| | | |
| 'wrongAsPath': 'wrong AS- | | |
| Path', | | |
| | | |
| 'lookingGlass': 'link to to the | | |
| Looking Glass used to verify AS- Path', | | |
| | | |
| 'le- galPrefix': 'legal prefix', | | |
| gairienx. legai prenx, | | |
| 'wrongPrefix': 'wrong | | |
| prefix' | | |
|)], | | |
| | | |
| 'malware': [{ | | |
| (an an a latter (12,10,20, 1 | | |
| 'sourceld': 'f34030ef- 358a- 445c-8567-25985ce6d91c', | | |
| | | |
| 'tar- | | |

| get': { | | |
|--|--|--|
| 00000 | | |
| 'ip': '127.0.0.1' | | |
| }, | | |
| " | | |
| 'sources': [{ 'ip': | | |
| | | |
| ʻ127.0.0.1', | | |
| | | |
| 'domain': 'example.com', | | |
| 'url': 'http://example.com' | | |
| <pre>in intp.//example.com }],</pre> | | |
| ,11, | | |
| 'classifications': [{ | | |
| | | |
| 'vendorName': 'name | | |
| of the MCSE tool, | | |
| | | |
| 'vendorVerdict': 'MC classification' | | |
| <pre>}],</pre> | | |
| ,11 | | |
| 'malwareSamples': | | |
| | | |
| [{ 'hash': { | | |
| | | |
| 'md5': '4BA5139A444538479D9D750E2E277 | | |
| 4BA5139A444538479D9D750E2E277 9BF', | | |
| | | |
| 'sha1': | | |
| 'D2B063763378A8CB38B192B2F71E7 | | |
| 8BC13783EFE', | | |
| | | |

| 'sha256': | | |
|---------------------------------|--|--|
| | | |
| 'E25059612A71BAB224C7CB438FD7A | | |
| 0D3C1C78AD40664C48F12A9AE48FA | | |
| | | |
| 441E44' | | |
| | | |
| | | |
| }, | | |
| | | |
| | | |
| 'attachment': { | | |
| · · · · · · · · · · | | |
| | | |
| 'sourceld': | | |
| | | |
| 'f34030ef- 358a-445c-8567- | | |
| 25985ce6d91c', | | |
| , | | |
| | | |
| 'comment | | |
| | | |
| ': 'attachment | | |
| description', | | |
| | | |
| | | |
| 'dateTimeAt': '2018- | | |
| | | |
| 03-22T08:14:38Z ', | | |
| | | |
| | | |
| 'file': { | | |
| | | |
| | | |
| 'name': 'file | | |
| | | |
| name', | | |
| | | |
| | | |
| 'size': 'file | | |
| size | | |
| | | |
| in bytes', | | |
| | | |
| | | |
| 'base64' | | |
| : 'attachment in | | |
| | | |
| base64 format' | | |
| | | |
| | | |
| }, | | |
| | | |
| | | |
| 'fileLink': | | |
| 'http://domain.com/archive.rar' | | |
| http://domain.com/archive.rai | | |
| | | |
| 1 | | |
| } | | |
| }], | | |
| | | |

| | | |
|--|------|--|
| 'malwareMessageSenders': [{ | | |
| 'email': 'qwerty@example.ru' | | |
| 'server': '127.0.0.1' | | |
|)], | | |
| <pre>'malwareMessageAttach- ment': {</pre> | | |
| ʻsourceld': 'f34030ef- 358a- 445c-8567-25985ce6d91c', | | |
| 'comment': 'comment to the attachment', | | |
| ʻdateTimeAt': '2018- 03- 22T08:14:38Z', | | |
| ʻfile': { | | |
| 'name': 'file name', | | |
| 'size': 'file size in bytes', | | |
| Base64 formate' 'attachment in base64 format' | | |
| }, | | |
| ʻfileLink': ʻhttp://domain.com/archive.rarʻ | | |
| }, | | |

| 'harmful Resource Address': | | |
|---|--|--|
| [{ 'ip': '127.0.0.1', | | |
| 'domain': 'example.com', | | |
| 'url': 'http://example.com' | | |
| <pre>un: http://example.com }],</pre> | | |
| 'iocs': [{ | | |
| 'net': [{ | | |
| | | |
| 'impact': 'type of the detected compromising identifier', | | |
| 'comment': | | |
| 'additional description', | | |
| }], | | |
| 'fil': [{ | | |
| 'impact': 'type of the | | |
| detected compromising identifier', | | |
| 'comment': 'additional description', | | |
| | | |
| 3], | | |
| 'reg': [{ | | |
| | | |

| 'impact': 'type of the detected compromising identifier', | | |
|--|--|--|
| 'comment': 'additional description', | | |
| 31. | | |
| 'prc': [{ 'impact': 'type of the | | |
| detected compromising identifier', | | |
| 'comment': 'additional description', | | |
| }], 'oth': [{ | | |
| 'impact': 'type of the detected compromising identifier', | | |
| 'comment': 'additional description', | | |
| }] }], | | |
| ʻin- fectionMethods': [{ | | |
| 'type': 'type of the suggested | | |
| | | |

| infection method', | | |
|-----------------------------------|--|--|
| | | |
| 'comment': 'additional | | |
| description' | | |
| }] | | |
| | | |
| }], | | |
| 'socialEngi- | | |
| neering': { | | |
| U V | | |
| 'sourceld': 'f34030ef- | | |
| | | |
| 358a- 445c-8567-25985ce6d91c', | | |
| | | |
| 'soiTypes': ['identifier of the | | |
| social engineering method'], | | |
| | | |
| 'soiSenders': [{ | | |
| | | |
| | | |
| 'phoneNumber': | | |
| '1212312345678', | | |
| | | |
| 'email': 'qwerty@example.ru' | | |
| | | |
| 'server': '127.0.0.1' | | |
| | | |
| 3], | | |
| | | |
| <pre>'messageAttachment': {</pre> | | |
| | | |
| 'sourceld': 'f34030ef- | | |
| | | |
| 259- | | |
| 358a- | | |
| 445c-8567-25985ce6d91c', | | |
| | | |
| 'comment': 'comment to | | |
| the attachment', | | |
| | | |
| 'dateTimeAt': '2018-03- | | |
| | | |



| 'assignment': 'purpose of the attacked object', |
|--|
| 'serviceType': 'type of the information service', |
| 'network': 'network address' |
| }, |
| 'at- tackType': { |
| 'type': 'attack type (by OSI levels)', |
| 'comment': 'additional description' |
| }, |
| 'sources': [{ 'ip': |
| <pre>'127.0.0.1' }],</pre> |
| 'power': { |
| 'pps': 'number of packets per second', |
| 'mps': 'number of megabits per second', |
| 'rps': 'number of requests per second', |
| }, |

| "startTimeAt": "2018- | | |
|--|--|--|
| 03- 22T08:14:38Z ", | | |
| "endTimeAt": "2018- | | |
| 03- 22T09:15:44Z ", | | |
| "neg- | | |
| ativeImpact": { | | |
| "type": 'negative impact | | |
| type', | | |
| "comment": 'comment to | | |
| the selected type' | | |
| } | | |
| }], | | |
| "atmAttacks": | | |
| { | | |
| "sourceld": "f34030ef- | | |
| 358a- 445c-8567-25985ce6d91c", | | |
| "tar- get": { | | |
| 8 | | |
| "type": 'attacked object | | |
| type','description': | | |
| | | |
| 'additional | | |
| description' | | |
| }, 'at- | | |
| tackType": [{ | | |
| | | |
| "type": 'attack type depending on the attached target', | | |
| acpending of the attached target, | | |

| 'additional description' | | |
|--------------------------------|--|--|
| }], | | |
| ʻat- | | |
| tackImage': { | | |
| | | |
| 'sourceld': 'f34030ef- | | |
| 358a- 445c-8567-25985ce6d91c', | | |
| 5388- 445C-8507-25985CE0051C, | | |
| | | |
| 'comment': 'comment to | | |
| the attachment', | | |
| | | |
| 'dateTimeAt': '2018- | | |
| 03- 22T08:14:38Z ', | | |
| | | |
| 'file': { | | |
| | | |
| 'name': 'file name', | | |
| | | |
| 'size': 'file size in | | |
| bytes', | | |
| | | |
| 'base64': | | |
| 'attachment in base64 format' | | |
| | | |
| }, | | |
| 1/ | | |
| 'fileLink': | | |
| 'http://domain.com/archive.rar | | |
| (| | |
| | | |
| } | | |
| }, | | |
| ʻvulnerabili | | |
| ties': [{ | | |
| | | |
| 'sourceld': 'f34030ef- | | |
| | | |

| 'additional description' | | |
|--|--------|--|
| | }], | |
| | 'at- | |
| tackImage': { | | |
| | | |
| 'sourceld': 'f34030ef 358a- 445c-8567-25985ce6d91 | | |
| 536d- 445t-6507-25965tebu91 | | |
| 'comment': 'comment | tto | |
| the attachment', | | |
| | | |
| 'dateTimeAt': '20: | 18- | |
| 03- 22T08:14:38Z ', | | |
| | | |
| ʻfile': { | | |
| 'name': 'file na | mol | |
| name. mena | ine, | |
| 'size': 'file size i | n | |
| bytes', | | |
| | | |
| 'base64': | | |
| 'attachment in base64 format' | | |
| }, | | |
| 17 | | |
| 'fileLink': | | |
| 'http://domain.com/archive.ra | r | |
| ' | | |
| | } | |
| }, | | |
| ʻvulner. | abili- | |
| ties': [{ | | |
| 'sourceld': 'f34030ef | | |
| 358a- 445c-8567-25985ce6d91 | | |
| | • | |

| 'tar- get': { | | |
|--|--|--|
| ʻip': '127.0.0.1', | | |
| 'domain': 'example.com', 'url' | | |
| 'http://example.com', | | |
| 'serviceType': 'information service type' }, | | |
| ر sources': [{ 'ip': | | |
| | | |
| ʻ127.0.0.1', | | |
| 'url': 'http://example.com' }], | | |
| 'identifier': 'vulnerability identifier', | | |
| 'cvss': 'CVSS metrics', | | |
| 'idCustom': { | | |
| 'description': 'vulnerability description' | | |
| 'swName': 'software name', | | |
| 'swVer': 'software version', | | |

| 'cweType': 'CWE error type', - | | |
|--|--|--|
| 'class': 'vulnerability class', | | |
| 'osName': 'operating system that controls software with detected vulnerability', | | |
| 'detectedAt': 'date and time when vulnerability is detected', | | |
| 'baseCVSS': 'baseline vector of vulnerability', | | |
| 'danger': 'hazard level of the detected vulnerability', | | |
| 'measures': 'possible measures to eliminate vulnerability', | | |
| 'status': 'vulnerability status', | | |
| 'exploit': 'existence of | | |
| exploit', - | | |
| 'recommendation': 'information on vulnerability elimination', | | |
| 'link': 'links to sources of information on the elimination of vulnerability', | | |

| 'manufacturer': 'a company | |
|----------------------------------|--|
| (organisation) that manufactures | |
| (develops) software in which a | |
| vulnerability has been detected' | |
| value ability has been detected | |
| } | |
| }], | |
| | |
| 'bruteForces': | |
| | |
| | |
| 'sourceld': 'f34030ef- | |
| 358a- 445c-8567-25985ce6d91c', | |
| | |
| 'tar- | |
| get': { | |
| | |
| (in/, (1)7,0,0,1/ | |
| ʻipʻ: ʻ127.0.0.1', | |
| | |
| 'url': 'http://example.com', | |
| | |
| | |
| 'serviceType': 'service type' | |
| }, | |
| | |
| 'sources': [{ | |
| sources . It | |
| | |
| ʻipʻ: ʻ127.0.0.1′ | |
| }], | |
| | |
| 'ac- | |
| countOs': { | |
| | |
| 'name': 'account name', | |
| | |
| | |
| | |
| 'privileges': 'level of | |
| (privilege) of account name' | |
| | |
| } | |
| | |

| | }], 'spams': [{ | | |
|------------|--|--|--|
| | | | |
| 358a | 'sourceld': 'f34030ef- - 445c-8567-25985ce6d91c', | | |
| | 're | | |
| - '2018 | ceivedAt': 3-03-22T08:14:38Z' <i>,</i> | | |
| gets' | tar- ۱ | | |
| Sec. | | | |
| | 'email': 'qwerty@example.ru' }], | | |
| | | | |
| | 'sources': [{ | | |
| | ʻip': | | |
| | ʻ127.0.0.1', | | |
| | 'domain': 'example.com', | | |
| | 'email': 'qwerty@example.ru' | | |
| | }], | | |
| | 'spamImages': { | | |
| 2582 | 'sourceld': 'f34030ef- - 445c-8567-25985ce6d91c', | | |
| 330a | | | |
| | 'comment': 'attachm | | |
| ent d | escription', | | |
| 03- 2 | 'dateTimeAt': '2018- 2T08:14:38Z', | | |
| | 'file'· { | | |

| 'name': 'file name', | | |
|------------------------------------|--|--|
| | | |
| 'size': 'file size in | | |
| bytes', | | |
| | | |
| 'base64': | | |
| 'attachment in base64 format' | | |
| attachment m baseb4 format | | |
| | | |
| }, | | |
| | | |
| 'fileLink': | | |
| 'http://domain.com/archive.rar | | |
| (| | |
| , | | |
| } | | |
| }], | | |
| 'con- | | |
| trolCenters': [{ | | |
| | | |
| 'sourceld': 'f34030ef- | | |
| 358a- 445c-8567-25985ce6d91c', | | |
| | | |
| 'tar- | | |
| get': { | | |
| | | |
| ʻip': '127.0.0.1', | | |
| | | |
| 'url': 'http://example.com' | | |
| | | |
| }, | | |
| | | |
| 'hostUrl': | | |
| 'http://example.com', | | |
| ʻin- | | |
| truderlp': '1.1.1.1', | | |
| 'in- | | |
| | | |
| truderActions': 'what preceded the | | |
| incident', | | |
| ʻde- | | |

| scription': 'known information | | |
|---|--|--|
| about the Botnet Command | | |
| Centre', | | |
| centre, | | |
| | | |
| 'nodes': [{ | | |
| 1100003 . [[| | |
| | | |
| 'ip': '127.0.0.1', | | |
| | | |
| | | |
| <pre>'lastRequestRateTimeA</pre> | | |
| t': '2018-03-22T08:08:49Z' | | |
| }] | | |
| | | |
| }], | | |
| 'sim': { | | |
| Siiii . { | | |
| | | |
| 'sourceld': 'f34030ef-358a- | | |
| 445c-8567-25985ce6d91c', | | |
| | | |
| 'mo- | | |
| bileOperator': 'mobile phone | | |
| operator name', | | |
| | | |
| | | |
| 'phoneNumber | | |
| ': '1212312345678' <i>,</i> | | |
| , | | |
| | | |
| 'imsi': 'unique SIM card | | |
| number', | | |
| 'im- | | |
| | | |
| siChangedAt': 'date when the IMSI | | |
| change was recorded' | | |
| }, | | |
| | | |
| ʻphish- | | |
| ingAttacks': [{ | | |
| | | |
| () (() () () () () () () () (| | |
| 'sourceId': 'f34030ef- | | |
| 358a- 445c-8567-25985ce6d91c', | | |
| 'tar- | | |
| | | |
| get': { | | |

| ʻip': '127.0.0.1', | |
|-------------------------------|--|
| | |
| 'domain': 'example.com' | |
| }, | |
| 'harmful': [{ 'ip': | |
| | |
| ʻ127.0.0.1', | |
| 'url': 'http://example.com' | |
|)], '' | |
| 'fixa - tionAt': | |
| '2018-03-22T08:08:49Z ', | |
| 'messageAttachment': { | |
| | |
| 'sourceld': 'f34030ef- | |
| 358a- | |
| 445c-8567-25985ce6d91c', | |
| 'comment': | |
| 'attachm | |
| ent description', | |
| 'dateTimeAt': '2018- | |
| 03- 22T08:08:49Z ', | |
| 'file': { | |
| | |
| 'name': 'file name', | |
| 'size': 'file size in | |
| bytes', | |
| 'base64': | |
| 'attachment in base64 format' | |



| | | |
|--|--|--|
| }], | | |
| ʻac- | | |
| tivityType': 'description of malicious | | |
| activity' | | |
| | | |
| }], | | |
| 'changeCon- | | |
| tent': [{ | | |
| | | |
| () (21020 (| | |
| 'sourceld': 'f34030ef- | | |
| 358a- 445c-8567-25985ce6d91c', | | |
| 'tar- | | |
| gets': [{ | | |
| • | | |
| ʻip': '127.0.0.1', | | |
| ip. 127.0.0.1, | | |
| | | |
| 'url': 'http://example.com' | | |
| }], | | |
| | | |
| 'type': 'type of content' | | |
| | | |
| }], | | |
| 'scanPorts': | | |
| [{ | | |
| | | |
| (| | |
| 'sourceld': 'f34030ef- | | |
| 358a- 445c-8567-25985ce6d91c', | | |
| | | |
| 'sources': [{ | | |
| | | |
| 'ip': 'IP address' | | |
| | | |
| }], | | |
| | | |
| 'ports': ['21'], | | |
| | | |
| 'method': 'information on | | |
| | | |
| scanning methods | | |

| or software used for this p | ourpose' | |
|-----------------------------|----------|--|
| | | |
| | '2018- | |
| 03- 22T08:08:49Z', | | |
| | | |
| | '2018- | |
| 03- 22T08:09:49Z' | | |
| }], | | |
| ʻoti | her': { | |
| | | |
| 'sourceld': 'f340 | | |
| 358a- 445c-8567-25985ce6 | 6d91c', | |
| | 'de- | |
| scription': 'computer attac | ck | |
| description', | | |
| to a superior to t | | |
| 'source': { | | |
| ʻip': ʻ127.0.0.1', | | |
| ip. 127.0.0.1, | | |
| 'url': 'http://example | com' | |
| | | |
| | }, | |
| 'type': 'other | tuna of | |
| prohibited, malicious, | | |
| content', | | |
| | 'at- | |
| tachment': { | | |
| | | |
| 'sourceld': 'f3403 | | |
| 445c-8567-25985ce6d91c' | , , | |
| | | |
| 'comment': | | |
| | 'attachm | |
| ent description', | | |

| ʻdateTimeAt': ʻ2018- 03- 22T08:08:49Z', | | |
|---|--|--|
| 'file': { | | |
| 'name': 'file name', | | |
| 'size': 'file size in bytes', | | |
| 'base64': 'attachment in base64 format' | | |
| λ. | | |
| ʻfileLink': ʻhttp://domain.com/archive.rar' | | |
| } | | |
| }, 'finalReport': { | | |
| ': 'date and time of incident closure' | | |
| 'recovery': 'incident recovery identifier', | | |
| 'description' : 'additional description if recovery is impossible', | | |
| 'rootCause': 'key causes of the incident', | | |
| 'mainActions': | | |

| 'actions taken to prevent future incidents', | | |
|--|--|--|
| 'signatures': [{ | | |
| | | |
| 'identifier': 'signature identifier', | | |
| 'name': 'detection tool', | | |
| 'source': 'signature source', | | |
| 'eventsAmount': 'number of signature activations' | | |
| }], 'snort': | | |
| ['rule1', 'rule2'], | | |
| 'attachment': { | | |
| 'sourceld': 'f34030ef- 358a- 445c-8567-25985ce6d91c', | | |
| 'comment': | | |
| 'attachm ent description', | | |
| 'dateTimeAt': '2018- 03- 22T08:14:38Z', | | |
| 'file': { | | |
| 'name': 'file name', | | |
| | | |

| bytes | size': 'file size in |
|---------|--------------------------------------|
| base6 | base64': 'attachment in ormat' |
| | }, |
| 'http:, | fileLink': omain.com/archive.rar' |
| | } } |
| 3 | |

Annex 2. Schemes of interaction between the Bank of Russia and an information exchange participant

| The form of distribution by the Bank of Russia among information exchange participants of data on the detected incidents associated with violations of data protection requirements | The form of a Bank of Russia request to an information exchange participant servicing the payee | The form of a Bank of Russia information message to an information exchange participant servicing the payer | The form of a Bank of Russia information message on imposing (or lifting) a restriction on bank (correspondent) accounts (sub- accounts) of information exchange participants in the form of a ban on debiting funds |
|--|--|--|--|
| { | { | { | { |
| 'header': { | 'header': { | 'header': { | 'header': { |
| 'schemaType': 'reaction', | 'schemaType': 'anti- | 'schemaType': | 'schemaType': 'lockRe- |
| 'schemaVersion': '1', | fraudRequest', | 'antifraudReturn', | sponse', |
| 'version': '1', | 'schemaVersion': '1', | 'schemaVersion': | 'schemaVersion': '1', |
| 'publishedAt': '2002- | 'version': '1', | '1', | 'version': '1', |
| 10- 02T15:00:00.05Z' | 'memberId': | 'version': '1', | 'memberId': '9527dd0c- |
| }, | '9527dd0c-0765-4f1c-8f5f- | 'memberld': | 0765-4f1c-8f5f-70a02cf4046c', |
| 'reaction': { | 70a02cf4046c', | '9527dd0c-0765-4f1c-8f5f- | 'sourceld': |
| 'fixationAt': '2002- | 'publishedAt': | 70a02cf4046c', | 'f34030ef |
| 10-02T15:00:00.05Z', | '2002- 10-02T15:00:00.05Z' | 'publishedAt': | - 358a-445c-8567-25985ce6d91c', |
| 'rootCause': 'key causes of the | }, | '2002-10-02T15:00:00.05Z' | 'publishedAt': '2002-10- |
| incident', | | | 02T15:00:00.05Z' |

| | | 'antifraudRequest': [{ | }, | }, |
|----------------|--|---------------------------------|---|---|
| | 'vectorCode': 'computer attack vector | 'sourceld': 'f34030ef- | 'anifraudReturn': [{ | 'lockResponse': [{ |
| identifier', | | 358a-445c-8567-25985ce6d91c', | 'sourceld': | 'sourceld': |
| | 'serviceType': [{ | 'victim': 'information on | 'f34030ef-358a-445c-8567- | (f34030ef |
| | 'type': type of the attacked | the legal status of the payer', | 25985ce6d91c', | - 358a-445c-8567-25985ce6d91c', |
| | object', | | ·victim': - | 'orgBik': '123456789', |
| | | 'payer': { | 'information on the legal status | 'regNumber': |
| | 'name': 'software/hardware | 'bik': | of the payer' | '123456789', |
| name', | | '123456789', | 'recipient': | 'uniqldentifier': |
| · | 'version': 'software/hardware | 'inn': | 'information on the legal status | '1234567891'. |
| version', | | '123456789000', | of the payee', | 'actionStatus': 'status |
| | 'description': 'additional | 'namePayer': | 'payer': { | of the restriction on funds debiting', |
| description o | f the type of the attacked object' | 'organisation name | 'bik': | coordinationStatus': |
| | }], | that is the payer', | '123456789', | |
| | 'typeOfAttack': 'computer attack type | 'payerTrans- | 'inn': | 'status of integrity control of the request to impose or lift the restriction |
| | code', | ferld': { | '123456789000', | |
| | | | ʻpay- | in the form of a ban on debiting funds', |
| | 'antifraudDestributed': [{ | 'transferType': type of money | erName': 'name of the | 'dateTimeAt': '2018-03- |
| | 'device': { | transfer method ', | organisation that is the payer', | 22T08:14:38Z', |
| | 'ip': '127.0.0.1', | | | 'text': 'additional |
| | 'imsi': 'international | | ʻpay- | description' |
| mohile subs | criber identifier (individual subscriber | 'paymentCard': { | erTransferId': { | 'attachment': { |
| number)', | | paymenteard . (| | 'sourceld' |
| number), | 'imei': 'international | 'number': | 'transferType': 'type of money | : 'f34030ef-358a-445c-8567- |
| mahila aquin | ment identifier', | ·123412341234123412', | transfer method', | 25985ce6d91c', |
| mobile equip | | 123412341234123412 , | | 'comment': |
| | 'aiic': 'acquiring insti- | 'sum': 'amount of | | 'attachment description', |
| tution identif | ication code (32 поле ISO 8583)', | the money transfer transactions | (a sum and Carrolly (| 'dateTimeAt |
| | 'cati': 'card acceptor | using payment cards', | 'paymentCard': { | ': '2018-03-22T08:14:38Z', |
| terminal iden | ntification (41 поле ISO 8583)', | using payment calus, | (auguala art) | 'file': { |
| | 'caic': 'card acceptor | 'currency': 'currency of a | 'number': | 'name': |
| identification | code (42 поле ISO 8583)' | money transfer transaction', | '123412341234123412', | 'file name', |
| | }, | | (| 'size': |
| | 'payee': { | | 'sum': the amount a money transfer transaction using | 'file size in bytes', |
| | ʻbik': '123456789', | | payment cards', | |
| | 'hash': | | payment calus, | 'base64': 'attachment in Base64 |
| | 71BAB224C7CB534FD7A0D3C1C78AD40 | | | format' |
| 64C48F12A9A | AE48FA441E11', | 13T09:14:38Z', | | } |
| | 'hashSnils': | | 'currency': 'currency of money | } |
| 'B49087832A | 71BAB224C7CB534FD7A0D3C1C78AD40 | 'rrn': 'the number generated | transfer transaction', | |
| 64C48F12A9A | AE48FA441E44', | | | |
| | 'inn': '123456789000'. | | | |

| 'transferId': { | for a money transfer transaction | | 11 |
|---|----------------------------------|----------------------------------|----|
| fansiend : { 'payment- | during its authorisation' | | }] |
| | - | 'dateTimeAt': '2018-01- | I |
| Card': { | }, 'set- | | |
| 'num- | | 13T09:14:38Z', | |
| ber': '123412341234123412' | tlement': { | 'rrn': 'the number | |
| }, (| 'number': | | |
| 'settlement': { | | generated for a money transfer | |
| 'num- | '12345123451234512345', | transaction during its | |
| ber': '12345123451234512345' | | authorisation' | |
| }, (-) | 'sum': 'amount of the money |) | |
| ʻpho- | transfer transaction', | }, | |
| neNumber': { | | (| |
| 'num- | 'currency': 'currency of the | 'settlement': | |
| ber': '1212312345678' | money transfer transaction', | ((assessible and) | |
| }, | | { 'number': | |
| 'idNumber': { | 'dateTimeAt': '2018- | '12345123451234512345', | |
| 'num | 01- 13T09:14:38Z' | | |
| - ber': | }, | 'sum': 'amount of the | |
| '1KoX6AA5VTdbBTkw27YEqKFaTtEQq97AAT' | | money transfer transaction', | |
| } | 'phoneNumber': { | | |
| } | | 'currency': 'currency of | |
| }, | 'number': '1212312345678', | the money transfer transaction', | |
| 'additionalStatus': { | | | |
| 'crossBorder' | 'sum': 'transaction amount', | 'dateTimeAt': '2018-01- | |
| : 'cross-border banking | | 13T09:14:38Z' | |
| identifier', | 'currency': 'currency of | | |
| 'additionalTransac- | | }, | |
| tionApprove': [| transaction | | |
| 'additional | - | 'phoneNumber': | |
| transaction approval identifier' | | | |
|] | 'dateTimeAt': '2018- | { 'number': | |
| } | 01- 13T09:14:38Z' | '1212312345678', | |
| }], | }, | | |
| 'impacts': { | ʻid- | 'sum': 'transaction | |
| 'trafficHijackAttacks': [{ | Number': { | amount', | |
| 'legalAsPath': | | - | |
| 'legal AS-Path', | 'number': | | |
| 'wrongAsPath': | '1KoX6AA5VTdbBTkw27YEqKFaTtEQq | | |
| 'wrongAsPath': | 97AAT', | currency', | |
| 'lookingGlass': | | | |
| 'Reference link to Looking Glass used to verify | | | |

| AS-Path', | 'sum': 'transaction amount', | | |
|---|--------------------------------------|----------------------------------|--|
| 'legalPrefix': 'legal | | | |
| prefix', | 'currency': 'currency of | 'dateTimeAt': '2018-01- | |
| 'wrongPrefix': | transaction | 13T09:14:38Z' | |
| wrongPrefix' | transaction | 13109.14.362 | |
| - | - | 1 | |
| }], | | }, | |
| 'malware': [{ | 'dateTimeAt': '2018- | | |
| 'sources': [{ | 01- 13T09:14:38Z' | 'idNumber': { | |
| ʻip': | } | | |
| '127.0.0.1', | }, | 'number': | |
| 'domain': | 'device': { | '1KoX6AA5VTdbBTkw27YEqKFaTt | |
| 'example.com', | ʻip': | EQq97AAT', | |
| 'url': | 'network address of the device', | | |
| 'http://example.com' | , | 'sum': 'transaction | |
| }], | 'imsi': 'international | amount', | |
| 'classifications': [{ | mobile subscriber identifier | - | |
| vendorName | (individual subscriber number)', | | |
| ': 'name of the MCSE tool used | (individual subscriber fullibery) | 'currency': 'transaction | |
| by the information exchange participant', | 'imei': 'international | currency', | |
| by the information exchange participant, | | currency, | |
| | mobile equipment identifier', | - | |
| 'vendorVerdict': 'MC class in accordance with | | | |
| the MCSE tool of the information exchange | 'aiic': 'Acquiring institution | 'dateTimeAt': '2018-01- | |
| participant' | identification code (32 поле | 13T09:14:38Z' | |
| }], | ISO 8583)', | } | |
| 'malwareSamples': [{ | | }, | |
| 'hash': { | 'cati': 'Card acceptor | 'device': | |
| 'md5': | terminal identification (41 поле ISO | { | |
| '4BA5139A444538479D9D750E2E2779BF', | 8583)', | | |
| 'sha1' | | 'ip': 'network address of | |
| | 'caic': 'Card acceptor identifi- | the device', | |
| D2B063763378A8CB38B192B2F71E78BC13783EFE ', | cation code (42 поле ISO 8583)' | | |
| , , , | } | 'imsi': 'international | |
| 'sha256': ' | }, | mobile subscriber identifier | |
| E25059612A71BAB224C7CB438FD7A0D3C1C78AD40 | | (individual subscriber number)', | |
| 64C48F12A9AE48FA441E44' | b payee . ('bik': | (martiadal subscriber hamber), | |
| · · · · · · · · · · · · · · · · · · · | '123456789', | 'imei': 'international | |
| }, (attachment): | | | |
| 'attachment': | | mobile equipment identifier', | |
| | '123456789000', | | |
| 'sourceld': 'f34030ef-358a-445c- | | 'aiic': 'Acquiring institu- | |
| 8567-25985ce6d91c', | | | |

| | 'payeeName': 'the name of | tion identification code (32 field | |
|---|--------------------------------------|------------------------------------|--|
| 'comment': 'comment to attachment', | the organisation that is the payee', | ISO 8583)', | |
| | 'payeeTrans- | | |
| 'dateTimeAt': '2018-03-22T08:14:38Z', | ferId': { | 'cati': 'Card acceptor | |
| 'file': { | | terminal identification (41 field | |
| ine. į | (two motory Type of a land on a set | | |
| (| 'transferType': 'money | ISO 8583)', | |
| 'name': 'file name', | transfer method type', | | |
| | | 'caic': 'Card acceptor | |
| 'size': 'file size in bytes', 'base64': | 'paymentCard': | identification code (42 field ISO | |
| | | 8583)' | |
| 'attachment in base64 format' | { 'number': | } | |
| }, | '123412341234123412' | }. | |
| 1) | }, | ,, 'payee': { | |
| (filelink': (http://domain.com/archive.row) | set- | bik': | |
| 'fileLink': 'http://domain.com/archive.rar' | | | |
| } | tlement': { | '123456789', | |
| }], | | ʻinn': | |
| 'malwareMessag- | 'number': 'the number of a | '123456789000', | |
| eSenders': [{ | settlement account of the payee | ʻpay- | |
| 'email': 'qwer- | opened with the money transfer | eeName': 'the name of the | |
| ty@example.ru', | operator serving the payee', | organisation that is the payee', | |
| 'server': | }, | 'payeeT- | |
| '127.0.0.1' | | ransferId': { | |
| }], | 'phoneNumber': { | | |
| 'malwareMes- | phonertumber . (| 'transferType': 'type of | |
| | 'number': '1212312345678' | | |
| sageAttachment': { | , | money transfer method', | |
| 'sourceld' | }, | (| |
| : 'f34030ef-358a-445c-8567-25985ce6d91c', | ʻid- | 'paymentCard': | |
| 'comment': | Number': { | | |
| 'comment to the attachment', | | { 'number': | |
| 'dateTimeAt': | 'number': | '123412341234123412', | |
| '2018-03-22T08:14:38Z', | '1KoX6AA5VTdbBTkw27YEqKFaTtEQc | | |
| ʻfile': { | 97AAT' | 'sum': 'amount of the | |
| | } | money transfer transaction | |
| 'name': 'file name', | } | using payment cards', | |
| 'size': | 1 | using payment cards , | |
| | }] | 'currency': ' currency of a | |
| 'file size in bytes', | 11 | money transfer | |
| | | transaction | |
| 'base64': 'attachment in base64 format' | | transaction | |
| }, | | | |

'fileLink': using payment cards'. 'http://domain.com/archive.rar' 'status1': { }, 'harmfulResourceAddress': [{ 'enrollment': ʻip': 'transaction suspension *'*127.0.0.1*'*, identifier', 'domain': 'example.com', 'dateTimeAt 'url': ': '2002-10-'http://example.com' 02T15:00:00.05Z' }], 'iocs': [{ 'net': [{ ʻim-}, pact': 'type of compromising identifier detected', 'settlement': 'comment': 'additional description' }], { 'number': 'fil': [{ '12345123451234512345', 'impact': 'type of compromising identifier detected', 'sum': 'amount of the money transfer transaction', 'comment': 'additional description' }], 'currency': 'currency of the money transfer transaction', 'reg': [{ 'impact': 'type of compromising identifier detected', 'status1': { 'comment': 'additional description' 'enrollment': 'transaction suspension }], 'prc': [{ identifier', 'impact': 'type of compromising identifier detected', 'dateTimeAt ': '2002-10-02T15:00:00.05Z'

| 'comment': 'additional description' | } |
|--|---|
| }], (++/- [[| , |
| 'oth': [{ 'im- | }, |
| pact': 'type of compromising identifier detected', | 'phoneNumber': |
| | |
| 'comment': 'additional description' | { 'number': |
| }] | ʻ1212312345678', |
| }], 'infectionMethod': [{ | 'sum': 'transaction |
| type': 'type | |
| of | - |
| Possible infection method', | |
| 'comment': | 'currency': 'transaction |
| 'comment to the selected type' | , currency', |
|)], }] | рации', |
| 'socialEngineering': { | 'status1': { |
| 'soiTypes': | |
| ['identifiers of social engineering methods'] | 'enrollment': |
| 'soiSenders': [{ | 'transaction suspension |
| 'pho- neNumber': '1212312345678', | identifier', |
| 'email': 'qwer- | 'dateTimeAt |
| ty@yandex.ru', | ·: '2002-10- |
| 'server': | 02T15:00:00.05Z' |
| '127.0.0.1' | |
| }], (massage Attach mont') | } |
| 'messageAttachment': { | b. |
| 'sourceld' | ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, |
| : 'f34030ef-358a-445c-8567-25985ce6d91c', | 'idNumber': { |
| 'comment': | (augusta) |
| 'attachment description', 'datetimeAt': | 'number': '1KoX6AA5VTdbBTkw27YEqKFaTt |
| '2018-03-22T08:14:38Z', | EQq97AAT', |
| 'file': { | |
| | 'sum': 'amount of the |
| 'name': 'file name', | transaction for changing the balance of funds', |
| | balance of funus , |
| | 'currency': 'currency of |




| 'http://example.com' | | |
|---|--|--|
| }], | | |
| 'identifier': | | |
| 'vulnerability identifier', | | |
| 'CVSS': ' | | |
| CVSS metrics' | | |
| | | |
| }], (havete Ferrers', [[| | |
| 'bruteForces': [{ | | |
| 'sources': [{ | | |
| ʻip': '127.0.0.1 | | |
| (| | |
| }] | | |
| }], | | |
| 'spams': [{ | | |
| 'receivedAt': '2018-03- | | |
| 22T08:14:38Z', | | |
| 'sources': [{ | | |
| ʻipʻ: | | |
| '127.0.0.1', | | |
| 'domain': | | |
| 'example.com', | | |
| 'email': 'qwer- | | |
| | | |
| ty@example.ru' | | |
|)], } | | |
| 'spamImages': { | | |
| 'sourceld' | | |
| : 'f34030ef-358a-445c-8567-25985ce6d91c', | | |
| 'comment': | | |
| 'comment to the attachment', | | |
| 'dateTimeAt': | | |
| '2018-03-22T08:14:38Z', | | |
| 'file': { | | |
| | | |
| 'name': 'file name', | | |
| 'size': | | |
| 'file size in bytes', | | |
| ,, | | |
| 'base64': 'attachment in base64 format' | | |
| }, | | |
| 17 | | |

| 'fileLink': | |
|---|--|
| 'http://domain.com/archive.rar' | |
| nttp.//uomain.com/archive.rai | |
| } | |
| }], | |
| 'controlCenters': [{ | |
| 'hostUrl': | |
| 'http://example.com', | |
| 'intruderlp': '1.1.1.1', | |
| 'intruderActions': | |
| 'what | |
| preceded the incident', | |
| 'description': | |
| 'additional description of the Botnet command | |
| centre', | |
| 'nodes': [{ | |
| ʻip': | |
| '127.0.0.1', | |
| 'lastReques- | |
| tRateTime': '2018-03-22T08:14:38Z ' | |
| }] | |
| }], | |
| 'sim': { | |
| 'mobileOperato | |
| r': 'name of a mobile telecom | |
| operator', | |
| 'phoneNumber': | |
| '1212312345678', | |
| 'imsi': 'unique | |
| SIM card number', | |
| 'imsiChangedAt': | |
| 2018-03-22T08:08:49Z ' | |
| }, | |
| 'prohibitedContents': [{ | |
| 'sources': [{ | |
| 'ip': | |
| '127.0.0.1', | |
| 'url': | |
| 'http://example.com' | |
| | |
| }], (turne's liturne of | |
| 'type': 'type of | |
| content' | |
| }], (phishingAttacks') [[| |
| 'phishingAttacks': [{ | |

| | | | |
|------------------------------|--|------|--|
| | 'harmful': [{ | | |
| | ʻip': | | |
| '127.0.0.1', | | | |
| | 'url': | | |
| 'http://example.com' | | | |
| | }], | | |
| | 'fixationAt': '2018-03- | | |
| 22T08:14:38Z', | | | |
| | 'messageAttachment': | | |
| { | Ŭ | | |
| · | 'sourceId' | | |
| : 'f34030ef-358a-445c-8567-2 | | | |
| | 'comment': | | |
| 'attachment description', | contraction of the second seco | | |
| attachment description ; | 'dateTimeAt': | | |
| '2018-03-22T08:14:38Z ', | date finicite . | | |
| 2010-03-22100.14.302 , | 'file': { | | |
| | ine . (| | |
| 'name': 'file name', | | | |
| name. me name, | 'size': | | |
| (file size in hytes) | Size . | | |
| 'file size in bytes', | | | |
| 'base64': 'attachmen | t in head () farment! | | |
| base64 : attachmen | | | |
| | }, | | |
| | ʻfileLink': | | |
| 'http://domain.com/archive. | rar | | |
| | } | | |
| }], | | | |
| 'malic | ciousResources': [{ | | |
| | 'sources': [{ | | |
| | ʻip': '127.0.0.1 | | |
| <i>i</i> , | | | |
| | 'url': | | |
| 'http://example.com' | | | |
| | }], | | |
| | 'activityType': 'type | | |
| | of | | |
| malicious activity' | | | |
| }], | | | |
| ʻchan | geContent': [{ | | |

| | / |
|------------------------------|-------------------------|
| | 'targets': [{ |
| | 'ip': |
| ʻ127.0.0.1', | |
| | 'url': |
| 'http://example.com' | |
| | }], |
| | 'type': 'type of |
| modified content' | |
| }], | |
| 'scanP | orts': [{ |
| | 'sources': [{ |
| | 'ip': |
| '127.0.0.1' | |
| | }], |
| | 'ports': ['23'], |
| | 'method': |
| | 'information on |
| scanning methods or software | |
| | 'startTimeAt': '2018- |
| 03-22T08:14:38Z', | |
| | 'endTimeAt': '2018-03- |
| 22T08:14:38Z' | |
| }], | |
| 'other' | ' : { |
| | 'description': |
| | 'description of |
| a computer attack', | |
| • | 'target': { |
| | 'ip': |
| '127.0.0.1', | |
| | 'url': |
| 'http://example.com' | |
| | }, |
| | 'type': 'type of |
| | content', 'attachment': |
| | { |
| | 'sourceld' |
| : 'f34030ef-358a-445c-8567-2 | |
| | 'comment': |
| 'comment to the attachment', | |
| | , 'dateTimeAt': |
| | daternitertt i |

| '2018-03-22T08:14:38Z', | | |
|---|--|--|
| 'file': { | | |
| | | |
| 'name': 'file name', | | |
| 'size': | | |
| | | |
| 'file size in bytes', | | |
| | | |
| 'base64': 'attachment in base64 format' | | |
| }, | | |
| 'fileLink': | | |
| 'http://domain.com/archive.rar' | | |
| 1 | | |
| ſ | | |
| , } | | |
| }, | | |
| 'mainActions': 'recommended | | |
| actions to counter a computer attack', | | |
| 'signatures': [{ | | |
| 'identifier': 'identifier of | | |
| signature', | | |
| 'yara': 'yara-rule', | | |
| 'snort': ['rule1', 'rule2'] | | |
| | | |
| }] | | |
| } | | |
| } | | |

STO BR BFBO-1.5-

Annex 3. Diagrams of processes of interaction between an information exchange participant and the Bank of Russia







Figure 2. An information exchange participant informs the Bank of Russia about incidents related to violation of data protection requirements

260

3.3 Scheme of informing the Bank of Russia by an information exchange participant about all money transfers and (or) attempts to make them without the customer's consent, as well as notification by money transfer operators of suspending funds crediting to the payee's bank account or increasing the payee's electronic funds balance, or of the impossibility to suspend funds crediting to the payee's bank account or increase the payee's electronic funds balance



3.4 Scheme of informing the Bank of Russia by information exchange participants other than the Bank of Russia structural units who uses express and non-rapid money money transfer services about imposing (or lifting) of the restriction on their bank (correspondent) accounts (sub-accounts) in the form of a ban on debiting funds in case of detection of incidents related to violation of the information protection requirements during money transfers at information infrastructure facilities of information exchange participants



262

3.5 Diagram of transmission by the Bank of Russia of information on detected incidents related to violation of data protection requirements to an information exchange participant



Dotted lines in Figures 1, 2, 3, 4 show messages and components that are not part of this standard.

The lines are given to represent the interaction between the information exchange participant and the Bank of Russia.

STO BR BFBO-1.5-2018

Bibliography

1. Federal Law No. 86-FZ, dated 10 July 2002, 'On the Central Bank of the Russian Federation (Bank of Russia)'.

2. Federal Law No. 161-FZ, dated 27 June 2011, 'On the National Payment System'.

3. Bank of Russia Regulation No. 382-P, dated 9 June 2012, 'On Requirements to Protect Information Related to Funds Transfers and on the Procedure for the Bank of Russia to Control the Compliance with Requirements to Protect Information Related to Funds Transfers'.

4. The Bank of Russia regulation establishing the forms and procedure for sending information by transfer operators, payment system operators, and payment infrastructure service providers to the Bank of Russia on all cases and attempts to make money transfers without the customer's consent and for receiving information from the Bank of Russia, contained in the database of cases and attempts to make money transfers without the customer's consent, and the procedure for taking measures by money transfer operators, payment system operators, and payment infrastructure service providers to counter money transfers without the customer's consent.

5. The Bank of Russia's regulation establishing mandatory requirements for credit institutions to ensure information protection during banking operations.

6. The Bank of Russia's regulation establishing mandatory requirements for non-bank financial institutions to ensure information protection in the course of financial market activities.

7. ISO 8583 – Financial transaction card originated messages – Interchange message specifications – Part 1: Messages, data elements and code values. URL: https://www.iso.org/obp/ui/#iso:std:iso:8583: – 1: ed-1: v1: en (reference date: 25 May 2018).

8. ISO 8583 – Financial transaction card originated messages – Interchange message specifications – Part 2: Application and registration procedures for Institution Identification Codes (IIC). URL: https://www.iso.org/obp/ui/#iso:std:iso:8583: – 2: ed-1: v1: en (reference date: 24 March 2018).

9. ISO 8583 – Financial transaction card originated messages – Interchange message specifications – Part 3: Maintenance procedures for messages, data elements and code values. URL: https://www.iso.or g/obp/ui/#iso:std:iso:8583: – 3: ed-1: v1: en (reference date: 17 April 2018).

10. ISO 4217 – Codes for the representation of currencies and funds. URL: https://www.iso.org/obp /ui/#iso:std:iso:4217: ed-8: v1: en (reference date: 25 February 2018).

11. RFC3339–DateandTimeontheInternet:Timestamps.URL:https://www.rfc-editor.org/rfc/rfc3339. txt (reference date: 02 February 2018).

12. RFC 791 – Internet Protocol. URL: https://www.rfc-editor.org/rfc/rfc791.txt (reference date: 14 May 2018).

13. RFC 5890 – Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework. URL: https://www.rfc-editor.org/rfc/rfc5890.txt (reference date: 08 February 2018).

14. RFC 1034 – Domain names – concepts and facilities. URL: https://www.rfc-editor.org/rfc/rfc1034. txt (reference date: 15 March 2018).

15. RFC 3986– Uniform Resource Identifier (URI): Generic Syntax. URL: https:// www.rfc-editor.org/rfc/rfc3986.txt (reference date: 07 March 2018).

16. RFC 4122 – A Universally Unique IDentifier (UUID) URN Namespace. URL: https:// www.rfc-editor.org/rfc/rfc4122.txt (reference date: 21 April 2018).

17. RFC 997 – Internet numbers. URL: https://www.rfc-editor.org/rfc/rfc997.txt (reference date: 23 January 2018).

18. RFC 5322 – Internet Message Format. URL: https://www.rfc-editor.org/rfc/rfc5322.txt (reference date: 24 January 2018).

19. National Standard of the Russian Federation GOST R ISO/IEC 15408-3-2013 'Information Technology. Security methods and tools. Criteria for assessing information technology security. Part 3. Security trust components'.

20. The Bank of Russia's regulation establishing the forms and procedure for money transfer operators to notify about the suspension of funds crediting to the payee's bank account or the increase in the payee's electronic funds balance, about the impossibility to suspend funds crediting to the payee's bank account or to suspend the increase in the payee's electronic funds balance.

21. The Bank of Russia's regulation establishing requirements for ensuring information protection in the Bank of Russia payment system.

22. Bank of Russia Regulation No. 595-P, dated 6 July 2017, 'On the Bank of Russia Payment System'.
23. ISO 8601:2004 – Data elements and interchange formats – Information interchange – Representation of dates and times. URL: https://www.iso.org/ru/standard/40 874.html (reference date: 29 June 2018).