

BANK OF RUSSIA STANDARD

STO BR BFBO-1.5-2023

# SAFETY OF FINANCIAL (BANKING) OPERATIONS

MANAGING INCIDENTS RELATED TO INFORMATION SECURITY THREATS AND OPERATIONAL RELIABILITY INCIDENTS

ON THE FORMS AND TERMS OF BANK OF RUSSIA'S COOPERATION WITH CREDIT INSTITUTIONS,

NON-BANKING FINANCIAL INSTITUTIONS AND NATIONAL PAYMENT SYSTEM SUBJECTS UPON DETECTION OF INCIDENTS

RELATED TO INFORMATION SECURITY THREATS AND OPERATIONAL RELIABILITY INCIDENTS

MOSCOW 2023

|  |  |
| --- | --- |
| 2 | STO BR BFBO-1.5-2023 |

## INTRODUCTION

1. DEVELOPED by the Bank of Russia.
2. ADOPTED AND ENACTED under Bank of Russia Order No. OD-215, dated 8 February 2023
3. TO SUPERSEDE STO BR BFBO-1.5–2018.

This Standard may not be fully or partially reproduced, circulated and distributed as an official edition without authorisation of the Central Bank of the Russian Federation.

|  |  |
| --- | --- |
|  |  |

TABLE OF CONTENTS

## [Introduction **2**](#_bookmark0)

## [Scope **5**](#_bookmark1)

## [Terms, definitions, designations and abbreviations **9**](#_bookmark2)

## [Bank of Russia's cooperation with information exchange participants **11**](#_bookmark3)

## [Methods of cooperation between the Bank of Russia and information exchange](#_bookmark4)

[participants **15**](#_bookmark4)

## [Cooperation between information exchange participants and the Bank of Russia](#_bookmark5)

## [in cases (or attempts) of funds transfers without consent of the client as well as in cases (or attempts) of carrying out of operations](#_bookmark5) [aimed at consummation of financial transactions using financial platform, not relying on the financial platform participant's will. **16**](#_bookmark5)

* 1. [Provision by information exchange participants - funds transfer operators, payment system operators, payment infrastructure service providers](#_bookmark5) [to the Bank of Russia of data about all cases and (or) attempts of funds transfer without the client's consent 16](#_bookmark5)
  2. [Provision by information exchange participants - electronic platform operators to the Bank of Russia of data about all cases and (or) attempts of funds transfers without the client's consent including information about nominal account](#_bookmark5) [operations without consent of the beneficiary client 16](#_bookmark5)
  3. [Provision by information exchange participants - financial platforms operators](#_bookmark5) [to the Bank of Russia of data about all cases and (or) attempts of carrying out of operations aimed at consummation of financial transactions using financial platform,](#_bookmark5) [not relying on the financial platform participant's will 16](#_bookmark5)
  4. [Request of the Bank of Russia for the purposes of identification of recipient of funds or payer 17](#_bookmark6)
  5. [Request of the Bank of Russia for the purposes of receiving data about the operation without consent based on information on any wrongful acts from the federal executive](#_bookmark6) [authority in the field of internal affairs 17](#_bookmark6)
  6. [Request of the Bank of Russia for the purposes of receiving data about acts of an information exchange](#_bookmark7) [participant rendering services to the recipient of funds 18](#_bookmark7)
  7. [Request of the Bank of Russia for the purposes of receiving information about payers to the](#_bookmark7) [funds recipient specified in the Bank of Russia' request 18](#_bookmark7)
  8. [Request of an information exchange participant in case of unreasonable provision](#_bookmark7) [to the Bank of Russia of information about transfers without the client's consent 18](#_bookmark7)
  9. [Request of the Bank of Russia on repeated provision of information about transfers without consent](#_bookmark8) [of the client 19](#_bookmark8)
  10. [Provision by information exchange participants of any additional and (or) more detailed data in respect of any information earlier submitted to the Bank of Russia 19](#_bookmark8)
  11. [Scheme of cooperation between the Bank of Russia and information exchange participants upon identification of cases and (or) attempts of funds transfers without the client's consent, as well as upon identification of cases and (or) attempts of operations aimed](#_bookmark8) [at consummation of financial transactions with the use of financial platform](#_bookmark8) [not relying on the financial platform participant's will 19](#_bookmark8)

## [Cooperation between information exchange participants and the Bank of Russia upon identification of information security incidents, in particular, unlawful disclosure of bank secret, personal data and (or) other data of clients or employees of an information exchange participant and operational reliability incidents **22**](#_bookmark9)

* 1. [List of types of information security incidents agreed with the federal executive authority liable for ensuring security and operational reliability incidents broken down by activities of credit institutions, non-banking financial institutions and national payment system subjects and their constituent](#_bookmark9) [technological processes 22](#_bookmark9)
  2. [Provision by information exchange participants of data about identification of an information](#_bookmark9)

[security incident 22](#_bookmark9)

* 1. [Provision by information exchange participants of data about identification of unlawful disclosure of bank secret and (or) protected information under regulatory acts of the Bank of Russia 23](#_bookmark10)
  2. [Provision by information exchange participants of data about the findings of investigation of an information security incident or unlawful disclosure of bank secret and (or)](#_bookmark10) [protected information under regulatory acts of the Bank of Russia 23](#_bookmark10)
  3. [Request of the Bank of Russia for the purposes of acknowledging the fact of unlawful disclosure of bank secret](#_bookmark11)

[and (or) protected information under regulatory acts of the Bank of Russia 24](#_bookmark11)

* 1. [Provision by information exchange participants of data about identification of an operational reliability incident 25](#_bookmark12)
  2. [Provision by information exchange participants of data about the findings of investigation of an operational reliability incident 25](#_bookmark12)

## [Cooperation between information exchange participants and the Bank of Russia upon identification of computer incidents, computer attacks and information security vulnerabilities **27**](#_bookmark13)

* 1. [List of computer incidents and computer attacks 27](#_bookmark13)
  2. [Provision by information exchange participants of data about computer incidents 27](#_bookmark13)
  3. [Provision by information exchange participants of data about computer attacks 28](#_bookmark14)
  4. [Provision by information exchange participants of data about identified information security vulnerabilities 29](#_bookmark15)
  5. [Request of the Bank of Russia to information exchange participants for the purposes of receiving data](#_bookmark16)

[about an identified computer attack or information security vulnerability 30](#_bookmark16)

* 1. [Request of the Bank of Russia for the purposes of receiving data about an information](#_bookmark16)

[exchange participant's ownership of an Internet resource 30](#_bookmark16)

* 1. [Scheme of cooperation between the Bank of Russia and information exchange participants upon identification of computer incidents, computer attacks and information security vulnerabilities 31](#_bookmark17)

## [Cooperation between information exchange participants and the Bank of Russia for the purposes of suspension/resumption of e-message exchange upon identification of information security incidents during funds transfers using ENTS at information infrastructure facilities of information exchange participants **32**](#_bookmark18)

## [Sending by information exchange participants to the Bank of Russia of information of the planned measures to disclose information about identified](#_bookmark19) [information security and operational reliability incidents ……………………………………………………………………………………......................................................**34**](#_bookmark19)

## [Appendices **35**](#_bookmark20)

## [References **293**](#_bookmark72)

## SCOPE

This standard governs the forms and the terms of cooperation between credit institutions, non-banking financial institutions and national payment system subjects (hereinafter collectively referred to as information exchange participants) and the Bank of Russia in cases provided for by Russian legislation, in particular, regulatory acts of the Bank of Russia.

The scope of application of this standard is determined under the requirements of Russian legislation, in particular, regulatory acts of the Bank of Russia providing for information exchange participants' responsibilities to inform the Bank of Russia:

* + of any identified cases and (or) attempts of funds transfers without consent of the client, of cases and (or) attempts of carrying out operations aimed at consummation of financial transactions using financial platform, not relying on the financial platform participant's will, information security incidents, in particular, unlawful disclosure of bank secret, personal data and (or) other data of clients or employees of an information exchange participant, computer incidents, computer attacks and information security vulnerabilities which may result in an information security or computer incident (hereinafter collectively referred to as incidents related to information security threats);
  + of operational risk events or a series of operational risk events cause by information security threats and (or) failure of information infrastructure facilities which resulted in failure to render or improper rendering of banking or financial services - operational risk events related to violation of operational reliability (hereinafter referred to as operational reliability incidents);
  + of the planned public events and measures to disclosure of information including press releases and holding press conferences, placement of information at the official websites on the Internet, in respect of identified information security and operational reliability incidents (herein after referred to as the planned information disclosure events).

This standard also applies in terms of information exchange with information exchange participants in accordance with the powers of the Bank of Russia to send requests and to obtain the required information about activity of information exchange participants under Russian legislation, in particular, regulatory acts of the Bank of Russia.

The object of this standard is as follows:

* Information about all cases and (or) attempts of funds transfers without the client's consent subject to requirements of:
  + Federal Law No. 161-FZ, dated 27 June 2011, ‘On the National Payment System’ (hereinafter, Federal Law No. 161-FZ) [3];
  + regulatory act of the Bank of Russia establishing the form and procedure of sending by funds transfer operators, payment system operators, payment infrastructure services operators, electronic platforms operators to the Bank of Russia of information about all cases and (or) attempts of funds transfers without the client's consent, form and procedure of receipt by them by the Bank of Russia of information contained in the database of cases and attempts of funds transfers without consent of the client as well as procedure of taking by funds transfer operators, payment system operators, payment infrastructure services operators, electronic platforms operators of events combating funds transfers without consent of the client developed based on parts 4, 6 and 7 of Article 27 of Federal Law No. 161-FZ [3].
* Information about all cases and (or) attempts of carrying out operations aimed at consummation of financial transactions using financial platform, not relying on the financial platform participant's will, subject to requirements of:
  + Federal Law No. 211-FZ, dated 20 July 2020, ‘On Consummation of Financial Transactions Using Financial Platform’ (hereinafter, Federal Law No. 211-FZ) [4];
  + regulatory act of the Bank of Russia establishing the form and procedure of sending by financial platform operators to the Bank of Russia of information about all cases and (or) attempts of carrying out operations aimed at consummation of financial transactions using financial platform, not relying on the financial platform participant's will, and receipt by financial platform operators, financial organisations from the Bank of Russia of information contained in the database of cases and attempts of carrying out operations aimed at consummation of financial transactions using financial platform, not relying on the financial platform participant's will as well as procedure of taking by financial platform operators of events to identify operations aimed at consummation of financial transactions using financial platform, not relying on the financial platform participant's will, and to combat consummation of such transactions based on parts 2, 4 and 5 of Article 12 of Federal Law No. 211-FZ [4].
* Information about identification of information security incidents, in particular unlawful disclosure

of bank secret, personal data and (or) other data of clients or employees of an information exchange participant, subject to requirements of:

* + the regulatory act of the Bank of Russia establishing binding requirements for lending institutions to ensure information security upon carrying out banking activity to combat funds transfers without consent of the client based on Article 57.4 of Federal Law No. 86-FZ. dated 10 July 2002, ‘On the Central Bank of the Russian Federation (Bank of Russia)’ (hereinafter, Federal Law No. 86-FZ) [1];
  + the regulatory act of the Bank of Russia establishing binding requirements for non-banking financial institutions to ensure information security upon carrying out activity in the field of financial markets to combat unlawful financial operations based on Article 76.4-1 of Federal Law No. 86-FZ [1];
  + the regulatory act of the Bank of Russia establishing requirements to ensure information security upon funds transfers and procedure of the Bank of Russia's monitoring compliance with requirements to ensure information security upon funds transfers based on part 3 of Article 27 of Federal Law No. 161-FZ [3].
* Information about identification of operational reliability incidents subject to requirements of:
  + the regulatory act of the Bank of Russia establishing binding requirements for credit institutions to operational reliability upon carrying out banking activity to ensure continuous provision of banking services based on Article 57.5 of Federal Law No. 86-FZ [1];
  + the regulatory act of the Bank of Russia establishing binding requirements for non-banking financial institutions to operational reliability upon carrying out activity in the field of financial markets to ensure continuous provision of financial services (other than banking services) based on Article 76.4-2 of Federal Law No. 86-FZ [1].
* Information about computer incidents, computer attacks and information security vulnerabilities subject to requirements of:
  + Federal Law No. 187-FZ, dated 26 July 2017, ‘On Security of the Critical Information Infrastructure of the Russian Federation’ (hereinafter, Federal Law No. 187-FZ) [2];
  + procedure for notifying a federal executive authority liable in the field of ensuring operation of the state system of identification, prevention and elimination of consequences of computer attacks affecting information resources of the Russian Federation, of computer incidents, response to them, measures to eliminate the consequences of computer attacks taken in respect of significant facilities of critical information infrastructure;
  + regulatory act of the Bank of Russia establishing the form and procedure of sending by funds transfer operators, payment system operators, payment infrastructure services operators, electronic platforms operators to the Bank of Russia of information about all cases and (or) attempts of funds transfers without the client's consent, form and procedure of receipt by them by the Bank of Russia of information contained in the database of cases and attempts of funds transfers without consent of the client as well as procedure of taking by funds transfer operators, payment system operators, payment infrastructure services operators, electronic platforms operators of events combating funds transfers without consent of the client developed based on parts 4, 6 and 7 of Article 27 of Federal Law No. 161-FZ [3].
* Information from information exchange participants using an express and non-express transfer service (hereinafter, ENTS) to transfer funds, of suspension/resumption of e-message exchange upon identification of information security incidents during funds transfers at information infrastructure facilities of information exchange participants, subject to requirements of the regulatory act of the Bank of Russia establishing requirements to information security within the Bank of Russia's payment system based on clause 19 of part 1 and part 9, Article 20 of Federal Law No. 161-FZ [3].
* Information about the planned measures to disclose information about identified information security and operational reliability incidents, subject to requirements of:
  + the regulatory act of the Bank of Russia establishing binding requirements for credit institutions to ensure information security upon carrying out banking activity to combat funds transfers without consent of the client based on Article 57.4 of Federal Law No. 86-FZ [1];
  + the regulatory act of the Bank of Russia establishing binding requirements for non-banking financial institutions to ensure information security upon carrying out activity in the field of financial markets to combat unlawful financial operations based on Article 76.4-1 of Federal Law No. 86-FZ [1];
  + the regulatory act of the Bank of Russia establishing requirements to ensure information security upon funds transfers and procedure of the Bank of Russia's monitoring compliance with requirements to ensure information security upon funds transfers based on part 3 of Article 27 of Federal Law No. 161-FZ [3];
  + the regulatory act of the Bank of Russia establishing binding requirements for credit institutions to operational reliability upon carrying out banking activity to ensure continuous provision of banking services based on Article 57.5 of Federal Law No. 86-FZ [1];
  + the regulatory act of the Bank of Russia establishing binding requirements for non-banking financial institutions to operational reliability upon carrying out activity in the field of financial markets to ensure continuous provision of financial services (other than banking services) based on Article 76.4-2 of Federal Law No. 86-FZ [1].

The provisions of this standard are not prescriptive in nature, unless an obligation to apply any of them is prescribed by the legislation of the Russian Federation or regulatory acts of the Bank of Russia. This standard may be used to include references thereto and (or) to directly include its provisions in internal documents of financial institutions as well as contracts and agreements entered into between institutions.

## TERMS, DEFINITIONS, DESIGNATIONS AND ABBREVIATIONS

This standard applies terms and definitions of the following acts of Russian legislation and standards:

* + in part of general terminology the terms and definitions of the National Standard of the Russian Federation GOST R 57580.3-2022 ‘Safety of Financial (Banking) Operations. Management of Information Security Threat Risk and Ensuring Operational Reliability. General Provisions’ (hereinafter referred to as GOST R 57580.3-2022) [13] and the National Standard of the Russian Federation GOST R 57580.1-2017 ‘Safety of Financial (Banking) Operations. Protection of Information of Financial Institutions. Basic Structure of Organisational and Technical Measures’ (hereinafter, GOST R 57580.1-2017) [12] are applied;
  + in part of identified cases and (or) attempts of funds transfers without the client's consent as well as suspension/resumption of e-message exchange upon identification of information security incidents during funds transfers at information infrastructure facilities of information exchange participants the terms and definitions of Federal Law No. 161-FZ shall apply [3];
  + in part of identified cases (or attempts) of carrying out of operations aimed at consummation of financial transactions using financial platform, not relying on the financial platform participant's will, the terms and definitions of Federal Law No. 211-FZ shall apply [4];
  + in part of identified operational reliability incidents terms and definitions of Bank of Russia Regulation No. 787-P, dated 12 January 2022, ‘On Binding Requirements for Credit Institutions to Operational Reliability upon Carrying out Banking Activity to Ensure Continuous Provision of Banking Services’ (hereinafter, Regulation No. 787-P of the Bank of Russia) [9] and Bank of Russia Regulation No. 779-P, dated 15 November 2021, ‘On Establishing Binding Requirements for Non-banking Financial Institutions to Operational Reliability upon Carrying out Activities Provided for by Part 1 of Article 76.1 of Federal Law No. 86-FZ, dated 10 July 2022, ‘On the Central Bank of the Russian Federation (Bank of Russia)’, to Ensure Continuous Provision of Financial Services (Other than Banking Services)’ (hereinafter, Regulation No. 779-P of the Bank of Russia) [10];
  + in part of identified computer incidents the terms and definitions of Federal Law No. 187-FZ shall apply [2].

This standard also uses the below designations and abbreviations:

AIPS FinTsERT means technical infrastructure (automated system) of the Bank of Russia;

AS ‘Feed-Anti-fraud’ means the Centralised database of cases and attempts of funds transfers without consent of the client;

TDB FSTEC means Information Security Threat Databank of the Federal Service for Technical and Export Control of Russia;

DB means database;

BIC means bank identification code;

Malware means malicious software;

RBS means remote banking service;

ID means identity document;

UBS means Unified Biometric System;

TIN means Taxpayer Identification Number;

CA means computer attack;

CI means computer incident;

CII means critical information infrastructure;

IPS means international payment system;

NCCCI means National Coordinating Center for Computer Incidents;

FTO means funds transfer operator;

EPO means electronic platform operator;

PS means payment system;

FPS means Faster Payments System;

Internet means information and telecommunications Internet network;

SNILS means individual insurance account number of an insured in the system of personalised registration of the Pension and Social Insurance Fund of the Russian Federation;

RSO means retail and service outlet;

NP means natural person;

LE means legal entity;

CAPEC – Common Attack Pattern Enumeration and Classification;

CPE – Common Platform Enumeration;

CVE – Common Vulnerabilities and Exposures;

CWE – Common Weakness Enumeration;

UI – User Interface;

URL – Uniform Resource Locator.

## BANK OF RUSSIA'S COOPERATION WITH INFORMATION EXCHANGE PARTICIPANTS

1. Information exchange participants notify the Bank of Russia of incidents related to information security threats, operational reliability incidents, of the planned measures to disclose information in cases provided for by Russian legislation, in particular, regulatory acts of the Bank of Russia.
2. Information exchange participants cooperate with the Bank of Russia using cooperation methods described in section 4.
3. The conditions and terms of notification of the Bank of Russia of incidents related to information security threats, operational reliability incidents, of the planned measures to disclose information as well as of sending responses to the Bank of Russia's requests shall be determined by this standard in part not governed by the legislation of the Russian Federation and the Bank of Russia.
4. This standard determines the forms of provision of data used to cooperate with the Bank of Russia in cases prescribed by Russian legislation, in particular, regulatory acts of the Bank of Russia, of sending to the Bank of Russia and receipt from the Bank of Russia of information (including as per form of notification of provision of information, form of notification of sending a request to exclude information, form of notification of provision a response to the request, form of notification of distributed data, form of notification of an event). The contents of the data provision forms sent to the Bank of Russia upon notification of incidents related to information security threats, operational reliability incidents, of the planned measures to disclose information as well as responses to the Bank of Russia's requests shall be determined in this standard.
5. This standard uses the below scheme of designating the data provision forms: <Type of data provision form>\_<Data provision form target>\_<Additional classification within the target>.

<Type of data provision form> may have the below designations:

* + NTF means the data provision form used by international exchange participants to notify the Bank of Russia. It does not provide for submitting a formalised response;
  + REQ means a form of request used by information exchange participants or the Bank of Russia to request information. Provides for submitting a binding formalised response;
  + RESP means a form of submitting a response to requests used by information exchange participants or the Bank of Russia to submit a formalised response to an information request.

<Data provision form target> may have the below designations:

* + OWC means a funds transfer without consent of the client or a transaction using financial platform, not relying on the financial platform participant's will;
  + ISI means information security incident;
  + ORI means operational reliability incident;
  + CI means computer incident;
  + CA means computer attack;
  + VLN means information security vulnerability;
  + IEP means information exchange participant.

<Additional classification within the target> depends on the data provision form target and is set forth in sections below.

1. Pre-filled data provision forms used in this standard constitute a particular case of data provision forms and relate to specific context (for instance, a type of operation, incident etc.). Pre-filled data provision forms may be used for notification of the Bank of Russia instead of basic data provision forms.
2. An obligation to fill in the fields of data provision forms depends on the below designations:
3. O - the field must be filled in;
4. CO - the field must be filled in, if the specific condition is met;
5. N - the field shall be filled in, where it is technically feasible to obtain the required information.
6. The fields of data provision forms must be filled in with data without the use of information concealment methods, in particular, encryption, masking or hashing, unless fill-in instructions otherwise specified.
7. The structure of data sent to the Bank of Russia, upon notification of incidents related to information security threats, operational reliability incidents, of the planned measures to disclose information, must not include information constituting state secret.

This standard describes the below data provision forms:

|  |  |  |
| --- | --- | --- |
| Code of data provision form | Name of data provision form | Section describing the data provision form |
| NTF\_OWC\_SNPS | Form of provision by information exchange participants - funds transfer operators, payment system operators, payment infrastructure service providers of data about all cases and (or) attempts of funds transfer without the client's consent | 5.1  Appendix 1 |
| NTF\_OWC\_OEP | Form of provision by information exchange participants - electronic platform operators of data about all cases and (or) attempts of funds transfers without the client's consent including information about nominal account operations without consent of the beneficiary client | 5.2  Appendix 2 |
| NTF\_OWC\_OFP | Form of provision by information exchange participants - financial platform operators of data about all cases and (or) attempts to carry out operations under financial transactions, not relying on the financial platform participant's will | 5.3  Appendix 3 |
| REQ\_OWC\_Identification RESP\_OWC\_Identification | Form of the Bank of Russia's request for the purposes of identification of the funds recipient or payer as well as form of submission of response to the Bank of Russia | 5.4  Appendix 4 |
| REQ\_OWC\_UUID RESP\_OWC\_UUID | Form of request of the Bank of Russia for the purposes of receiving data about the operation without consent based on information on any wrongful acts from the federal  executive authority in the field of internal affairs as well as form of submission of  response to the Bank of Russia | 5.5  Appendix 5 |
| REQ\_OWC\_Forward RESP\_OWC\_Forward | Form of the Bank of Russia's request for the purposes of receiving data about acts of an information exchange participant rendering services to the funds recipient to transfer funds as well as form of submission of response to the Bank of Russia | 5.6  Appendix 6 |
| REQ\_OWC\_Reverse RESP\_OWC\_Reverse | Form of request of the Bank of Russia for the purposes of receiving information about payers to the funds recipient specified in the Bank of Russia' request as well as form of submission of response to the Bank of Russia | 5.7  Appendix 7 |
| REQ\_OWC\_Review RESP\_OWC\_Review | Form of request of an information exchange participant in case of unreasonable submission to the Bank of Russia of information on transfers without consent of the client as well as form of submission of response of the Bank of Russia | 5.8  Appendix 8 |
| REQ\_OWC\_Correction RESP\_OWC\_Correction | Form of the Bank of Russia's request on repeated submission of information about transfers without consent of the client as well as form of submission of response to the Bank of Russia | 5.9  Appendix 9 |
| NTF\_OWC\_DataUpdate | Form of provision by information exchange participants of additional and (or) more detailed data in respect of any earlier submitted information about transfers without consent of the client | 5.10  Appendix 10 |
| NTF\_ISI\_Detect | Form of provision by information exchange participants of data about identification of an information security incident | 6.2  Appendix 12 |

|  |  |  |
| --- | --- | --- |
| NTF\_ ISI \_DataLeak | Form of provision by information exchange participants of data about identification of unlawful disclosure of bank secret and (or) protected information under regulatory acts of the Bank of Russia | 6.3  Appendix 13 |
| NTF\_ISI\_Investigation | Form of provision by information exchange participants of data about the findings of investigation of an information security incident or unlawful disclosure of bank secret and (or) protected information under regulatory acts of the Bank of Russia | 6.4  Appendix 14 |
| REQ\_ ISI \_DataLeak RESP\_ ISI \_DataLeak | Form of the Bank of Russia's request for the purposes of acknowledging the fact of unlawful disclosure of bank secret and (or) protected information under regulatory acts of the Bank of Russia | 6.5  Appendix 15 |
| NTF\_ORI\_Detect | Form of provision by information exchange participants of data about identification of an operational reliability incident | 6.6  Appendix 16 |
| NTF\_ORI\_Investigation | Form of provision by information exchange participants of data about the findings of investigation of an operational reliability incident | 6.7  Appendix 17 |
| NTF\_CI | Form of provision by information exchange participants of data about computer incidents | 7.2  Appendix 19 |
| NTF\_CA | Form of provision by information exchange participants of data about computer attacks | 7.3  Appendix 21 |
| NTF\_VLN | Form of provision by information exchange participants of data about identified information security vulnerabilities | 7.4  Appendix 23 |
| REQ\_IEP\_Detect RESP\_IEP\_Detect | Form of the Bank of Russia's request for the purposes of receiving information of an identified computer attack or an information security vulnerability as well as form of submission of response to the Bank of Russia | 7.5  Appendix 24 |
| REQ\_IEP\_IsWebSite RESP\_IEP\_IsWebSite | For of the Bank of Russia's request for the purposes of receiving data about an information exchange participant's ownership of an Internet resource as well as form of submission of response to the Bank of Russia | 7.6  Appendix 25 |
| REQ\_IEP\_CorrAccLock RESP\_IEP\_CorrAccLock | Form of request of an information exchange participant using ENTS to transfer funds for the purposes of suspension/resumption of e-message exchange upon identification of information security incidents during funds transfers using ENTS at information infrastructure facilities of information exchange participants as well as form of submission of response of the Bank of Russia | 8  Appendix 26 |
| NTF\_IEP\_Publication | Form of submission by information exchange participants of information of the planned measures to disclose information about identified information security or operational reliability incidents | 9  Appendix 27 |

To adopt a decision on notification an information exchange participant may use a decision-making scheme for decisions about notification of the Bank of Russia

FIG. 1. DECISION-MAKING SCHEME FOR DECISIONS ABOUT NOTIFYING THE BANK OF RUSSIA ABOUT INFORMATION SECURITY THREAT EVENTS



## METHODS OF COOPERATION BETWEEN THE BANK OF RUSSIA AND INFORMATION EXCHANGE PARTICIPANTS

The Bank of Russia and information exchange participants cooperate using technical infrastructure (automated system) of the Bank of Russia - AIPS FinTsERT.

In case cooperation between information exchange participants and the Bank of Russia using AIPS FinTsERT is not technically feasible:

* + information exchange participants must send information to the Bank of Russia using contact information of FinTsERT placed at the official website of the Bank of Russia in the information and telecommunications Internet network. Information sent using contact information of FinTsERT must be repeatedly sent to the Bank of Russia upon recovery of technical feasibility of cooperation between information exchange participants and the Bank of Russia using AIPS FinTsERT;
  + The Bank of Russia sends requests to information exchange participants using contact information provided by an information exchange participant in the participant's card1.

1 Form of AIPS FinTsERT containing information about information exchange participant.

## COOPERATION BETWEEN INFORMATION EXCHANGE PARTICIPANTS AND THE BANK OF RUSSIA IN CASES (OR ATTEMPTS) OF FUNDS TRANSFERS WITHOUT CONSENT OF THE CLIENT AS WELL AS IN CASES (OR ATTEMPTS) OF OPERATIONS AIMED AT CONSUMMATION OF FINANCIAL TRANSACTIONS USING FINANCIAL PLATFORM, NOT RELYING ON THE FINANCIAL PLATFORM PARTICIPANT'S WILL

* 1. PROVISION BY INFORMATION EXCHANGE PARTICIPANTS - FUNDS TRANSFER OPERATORS, PAYMENT SYSTEM OPERATORS, PAYMENT INFRASTRUCTURE SERVICE PROVIDERS TO THE BANK OF RUSSIA OF DATA

ABOUT ALL CASES AND (OR) ATTEMPTS OF FUNDS TRANSFER WITHOUT THE CLIENT'S CONSENT

Events, upon occurrence whereof information exchange participants - funds transfer operators, payment system operators, payment infrastructure service providers must send to the Bank of Russia data about all cases and (or) attempts of funds transfers without the client's consent (hereinafter, the information about transfers without consent of the client) as well as terms of submission of the specified information are established in the regulatory act of the Bank of Russia under parts 4, 6 and 7 of Article 27 of Federal Law No. 161-FZ [3].

Form of provision by information exchange participants - funds transfer operators, payment system operators, payment infrastructure service providers of data about transfers without consent of the client (*NTF\_OWC\_SNPS*) to the Bank of Russia is set forth in [Appendix 1](#_bookmark21) to this standard.

* 1. PROVISION BY INFORMATION EXCHANGE PARTICIPANTS - ELECTRONIC PLATFORM OPERATORS TO THE BANK OF RUSSIA OF DATA ABOUT ALL CASES AND (OR) ATTEMPTS OF FUNDS TRANSFERS WITHOUT THE CLIENT'S

CONSENT INCLUDING INFORMATION ABOUT NOMINAL ACCOUNT OPERATIONS WITHOUT CONSENT OF THE BENEFICIARY CLIENT

Events, upon occurrence whereof information exchange participants - electronic platform operators must send to the Bank of Russia data about all cases and (or) attempts of funds transfers without the client's consent including information about nominal account operations without consent of the beneficiary client (hereinafter, the information about transfers without consent of the client including information about nominal account operations without consent of the beneficiary client) as well as terms of submission of the specified information are established in the regulatory act of the Bank of Russia under parts 4, 6 and 7 of Article 27 of Federal Law No. 161-FZ [3].

Form of provision by information exchange participants - electronic platform operators of information about transfers without consent of the client including information about nominal account operations without consent of the beneficiary client (*NTF\_OWC\_OEP*) to the Bank of Russia is set forth in [Appendix 2](#_bookmark22) to this standard.

* 1. PROVISION BY INFORMATION EXCHANGE PARTICIPANTS - FINANCIAL PLATFORM OPERATORS TO THE BANK OF RUSSIA OF DATA ABOUT ALL CASES AND (OR) ATTEMPTS OF CARRYING OUT OF OPERATIONS AIMED AT CONSUMMATION OF FINANCIAL TRANSACTIONS USING FINANCIAL PLATFORM, NOT RELYING ON THE FINANCIAL PLATFORM PARTICIPANT'S WILL

Events, upon occurrence whereof information exchange participants - financial platform operators must send to the Bank of Russia data about all cases and (or) attempts of carrying out of operations aimed at consummation of financial transactions using financial platform, not relying on the financial platform participant's will (hereinafter, operations under financial transactions, not relying on the financial platform participant's will),

as well as terms of submission of the specified information are established in the regulatory act of the Bank of Russia under parts 2, 4 and 5 of Article 12 of Federal Law No. 211-FZ.

Form of provision by information exchange participants - financial platform operators of data about all cases and (or) attempts of carrying out operations under financial transactions, not relying on the financial platform participant's will (*NTF\_OWC\_OFP*) to the Bank of Russia is set forth in [Appendix 3](#_bookmark23) to this standard.

* 1. REQUEST OF THE BANK OF RUSSIA FOR THE PURPOSES OF IDENTIFICATION OF RECIPIENT OF FUNDS OR PAYER

Request of the Bank of Russia to an information exchange participant is sent by the Bank of Russia upon receipt from the information exchange participant of the notification containing information about transfers without consent of the client, for the purposes of identification of recipient of funds or payer under parts 4, 6 and 7 of Article 27 of Federal Law No. 161-FZ [3].

Upon receipt of a request for the purposes of identification of recipient of funds or payer information exchange participants send information to the Bank of Russia within the time frames established by the regulatory act of the Bank of Russia under parts 4, 6 and 7 of Article 27 of Federal Law No. 161-FZ [3].

Form of request of the Bank of Russia sent to an information exchange participant for the purposes of identification of recipient of funds or payer (*REQ\_OWC\_Identification*) as well as form of submission of response to the Bank of Russia containing information identifying the recipient of funds or payer (*RESP\_OWC\_Identification*) are set forth in [Appendix 4](#_bookmark24) to this standard.

* 1. REQUEST OF THE BANK OF RUSSIA FOR THE PURPOSES OF RECEIVING DATA ABOUT THE OPERATION WITHOUT CONSENT BASED ON INFORMATION ON ANY WRONGFUL

ACTS FROM THE FEDERAL EXECUTIVE AUTHORITY IN THE FIELD OF INTERNAL AFFAIRS

The Bank of Russia's request to a funds transfer operator (notification from the Bank of Russia) shall be sent by the Bank of Russia upon receipt from the federal executive authority in the field of internal affairs of information about committed wrongful acts.

Upon receipt of the request the funds transfer operator shall send the following data provision forms within the specified time frames:

* data provision form *NTF\_OWC\_SNPS* within the terms established in the regulatory act of the Bank of Russia under parts 4, 6 and 7 of Article 27 of the Federal Law

No. 161-FZ [3], in case of classification of the funds transfer operation, information whereof was received from the Bank of Russia based on information of the federal executive authority in the field of internal affairs about committed wrongful acts as an operation without consent of the client;

* form *RESP\_OWC\_UUID* within a business day following the date of receipt of the Bank of Russia's request, in case based on information from the Bank of Russia's request the funds transfer operation was not classified as an operation without consent of the client, or the data provision form *NTF\_OWC\_SNPS* on the respective operation had been earlier sent to the Bank of Russia.

Form of the Bank of Russia's request sent to a funds transfer operator, for the purposes of receipt of data about an operation without consent (*REQ\_OWC\_UUID*), as well as form of submission of response to the Bank of Russia (*RESP\_OWC\_UUID*), sent in cases provided for by paragraph 4, section 5.5 of this standard, are set forth in [Appendix 5](#_bookmark25) to this standard.

* 1. REQUEST OF THE BANK OF RUSSIA FOR THE PURPOSES OF RECEIVING DATA ABOUT ACTS

OF AN INFORMATION EXCHANGE PARTICIPANT RENDERING SERVICES TO THE RECIPIENT OF FUNDS TO TRANSFER FUNDS

The Bank of Russia's request to an information exchange participant rendering services to the recipient of funds shall be sent by the Bank of Russia upon receipt of the notification or information about funds transfer without consent of the client for the purposes of receiving information about acts of subsequent funds transfer by the recipient of funds under parts 4, 6 and 7 of Article 27 of Federal Law No. 161-FZ [3].

Upon receipt of the Bank of Russia's request the information exchange participant rendering services ti the recipient of funds shall send the information about acts of subsequent funds transfer of the recipient of funds to the Bank of Russia within the terms established in the regulatory act of the Bank of Russia under parts 4, 6 and 7 of Article 27 of Federal Law No. 161-FZ [3].

Form of request of the Bank of Russia sent to an information exchange participant rendering services to the recipient of funds for the purposes of receiving data about its funds transfer acts (*REQ\_OWC\_Forward*), as well as form of submission of response to the Bank of Russia containing information about acts of the information exchange participant to transfer funds (*RESP\_OWC\_Forward*), are set forth in [Appendix 6](#_bookmark26) to this standard.

* 1. REQUEST OF THE BANK OF RUSSIA FOR THE PURPOSES OF RECEIVING INFORMATION ABOUT PAYERS TO THE FUNDS RECIPIENT SPECIFIED IN THE BANK OF RUSSIA' REQUEST

The Bank of Russia's request to an information exchange participant rendering services to the recipient of funds shall be sent by the Bank of Russia upon receipt from the information exchange participant of the notification or information about funds transfer without consent of the client for the purposes of receiving information about payers to the specified funds recipient under parts 4, 6 and 7 of Article 27 of Federal Law No. 161-FZ [3].

Upon receipt of the Bank of Russia's request the information exchange participant rendering services to the recipient of funds shall send the information about payers to the specified funds recipient to the Bank of Russia within the terms established in the regulatory act of the Bank of Russia under parts 4, 6 and 7 of Article 27 of Federal Law No. 161-FZ [3].

Form of request of the Bank of Russia sent to an information exchange participant rendering services to the recipient of funds for the purposes of receiving information about payers to the specified funds recipient (*REQ\_OWC\_Reverse*), as well as form of submitting a response to the Bank of Russia containing information about payers to the specified funds recipient (*RESP\_OWC\_ Reverse*), are set forth in [Appendix 7](#_bookmark27) to this standard.

* 1. REQUEST OF AN INFORMATION EXCHANGE PARTICIPANT IN CASE OF

UNREASONABLE PROVISION TO THE BANK OF RUSSIA OF INFORMATION ABOUT TRANSFERS WITHOUT THE client'S CONSENT

Request of an information exchange participant shall be sent to the Bank of Russia upon identification under the risk management system implemented by the information exchange participant of cases of unreasonable provision of information about transfers without the client's consent under an earlier notification sent to the Bank of Russia under parts 4, 6 and 7 of Article 27 of Federal Law No. 161-FZ [3].

Following the results of consideration of the request the Bank of Russia shall send to the information exchange participant the information on consideration of the request.

Form of request of an information exchange participant sent to the Bank of Russia in case of unreasonable provision to the Bank of Russia of information about transfers without consent of the client (*REQ\_OWC\_Review*), as well as form of submission of response to the information exchange participant used by the Bank of Russia (*RESP\_OWC\_Review*), are set forth in [Appendix 8](#_bookmark28) to this standard.

* 1. REQUEST OF THE BANK OF RUSSIA ON REPEATED PROVISION OF INFORMATION ABOUT TRANSFERS WITHOUT CONSENT OF THE CLIENT

The Bank of Russia's request to an information exchange participant shall be sent by the Bank of Russia upon receipt from the information exchange participant of the notification or information about funds transfer without consent of the client for the purposes of receiving more detailed data to the information about transfers without consent of the client earlier submitted to the Bank of Russia under parts 4, 6 and 7 of Article 27 of Federal Law No. 161-FZ [3].

Upon receipt of the Bank of Russia's request the information exchange participant shall send repeated information about transfers without consent of the client within the terms established in the regulatory act of the Bank of Russia under parts 4, 6 and 7 of Article 27 of Federal Law No. 161-FZ [3].

Form of request of the Bank of Russia sent to the information exchange participant, about repeated provision of information about transfers without consent of the client (*REQ\_OWC\_Correction*), as well as form of submission of response to the Bank of Russia containing repeated information about transfers without consent of the client (*RESP\_OWC\_Correction*), are set forth in [Appendix 9](#_bookmark29) to this standard.

* 1. PROVISION BY INFORMATION EXCHANGE PARTICIPANTS

OF ANY ADDITIONAL AND (OR) MORE DETAILED DATA IN RESPECT OF ANY INFORMATION EARLIER SUBMITTED TO THE BANK OF RUSSIA

Conditions, upon occurrence whereof the information exchange participants send to the Bank of Russia any additional and (or) more detailed data to the information earlier submitted to the Bank of Russia as well as terms of submission of the specified information are established in the regulatory act of the Bank of Russia under parts 4, 6 and 7 of Article 27 of the Federal Law.

No. 161-FZ [3].

Form of provision by information exchange participants of any additional and (or) more detailed data to the earlier submitted information about transfers without consent of the client to the Bank of Russia (*NTF\_OWC\_DataUpdate*) is set forth in [Appendix 10](#_bookmark30) to this standard.

This form is targeted at updating the information in the database about cases and attempts of funds transfers without consent of the client:

* + - closing a bank account;
    - cessation of payment card use;
    - termination of a mobile telephone communications subscription agreement;
    - cessation of electronic payment facility use;
    - change of identity document number;
    - change of mobile telephone communications subscriber's number.
  1. SCHEME OF COOPERATION BETWEEN THE BANK OF RUSSIA AND INFORMATION EXCHANGE PARTICIPANTS UPON IDENTIFICATION OF CASES AND (OR) ATTEMPTS OF FUNDS TRANSFERS WITHOUT THE CLIENT'S CONSENT, AS WELL AS UPON IDENTIFICATION OF CASES

AND (OR) ATTEMPTS OF OPERATIONS AIMED AT CONSUMMATION OF FINANCIAL TRANSACTIONS USING FINANCIAL PLATFORM, NOT RELYING ON

THE FINANCIAL PLATFORM PARTICIPANT'S WILL

Scheme of cooperation between the Bank of Russia and information exchange participants upon identification of cases and (or) attempts of funds transfers without the client's consent, as well as upon identification of cases and (or) attempts of operations aimed at consummation of financial transactions using financial platform, not relying on the financial platform participant's will, is shown on Fig. 2.

Scheme of cooperation between the Bank of Russia and funds transfer operators due to receipt by the Bank of Russia of Information on any wrongful acts from the federal executive authority in the field of internal affairs, is shown on Fig. 3.

FIG. 2. SCHEME OF COOPERATION BETWEEN THE BANK OF RUSSIA AND INFORMATION EXCHANGE PARTICIPANTS UPON IDENTIFICATION OF CASES AND (OR) ATTEMPTS OF FUNDS TRANSFERS WITHOUT THE CLIENT'S CONSENT, AS WELL AS UPON IDENTIFICATION OF CASES AND (OR) ATTEMPTS OF OPERATIONS AIMED AT CONSUMMATION OF FINANCIAL TRANSACTIONS USING FINANCIAL PLATFORM, NOT RELYING ON THE FINANCIAL PLATFORM PARTICIPANT'S WILL



FIG. 3. SCHEME OF COOPERATION BETWEEN THE BANK OF RUSSIA AND FUNDS TRANSFER OPERATORS DUE TO RECEIPT BY THE BANK OF RUSSIA OF INFORMATION ON ANY WRONGFUL ACTS FROM THE FEDERAL EXECUTIVE AUTHORITY IN THE FIELD OF INTERNAL AFFAIRS



## COOPERATION BETWEEN INFORMATION EXCHANGE PARTICIPANTS AND THE BANK OF RUSSIA UPON IDENTIFICATION OF INFORMATION SECURITY INCIDENTS, IN

PARTICULAR, UNLAWFUL DISCLOSURE OF BANK SECRET, PERSONAL DATA AND (OR) OTHER DATA OF CLIENTS OR EMPLOYEES OF AN INFORMATION

EXCHANGE PARTICIPANT AND OPERATIONAL RELIABILITY INCIDENTS

* 1. LIST OF TYPES OF INFORMATION SECURITY INCIDENTS AGREED WITH THE FEDERAL EXECUTIVE AUTHORITY LIABLE

FOR ENSURING SECURITY AND OPERATIONAL RELIABILITY INCIDENTS BROKEN DOWN BY ACTIVITIES OF CREDIT INSTITUTIONS, NON-BANKING FINANCIAL INSTITUTIONS AND NATIONAL PAYMENT SYSTEM SUBJECTS AND THEIR CONSTITUENT TECHNOLOGICAL PROCESSES

Information exchange participants under paragraph eight of clause 8 of Bank of Russia Regulation No. 683-P, dated 17 April 2019, ‘On Establishing Binding Requirements for Credit Institutions to Information Security upon Carrying out Banking Activity to Combat Funds Transfers Without Consent of the Client’ (hereinafter, Regulation No. 683-P of the Bank of Russia) [5], paragraph two of clause 1.15 of Bank of Russia Regulation No. 757-P, dated 20 April 2021, ‘On Establishing Binding Requirements for Non-banking Financial Institutions to Ensure Information Security upon Carrying out Activity in the Field of Financial Markets to Combat Unlawful Financial Operations’ (hereinafter, Regulation No. 757-P of the Bank of Russia) [7], paragraph two of clause 1.5 of Bank of Russia Regulation No. 719-P, dated 4 June 2020,

‘On Requirements to Information Security upon Funds Transfers and on the Procedure of the Bank of Russia's Control over Compliance with Requirements to Information Security upon Funds Transfers’ (hereinafter, Regulation No. 719-P of the Bank of Russia) [6] must notify the Bank of Russia of identified information security incidents included in the list of types of incidents agreed with the federal executive authority authorised in the field of ensuring security.

Information exchange participants under paragraph two, clause 11 of Regulation No. 787-P of the Bank of Russia [9], paragraph two, clause 1.15 of Regulation No. 779-P of the Bank of Russia [10] must notify the Bank of Russia of identified operational reliability incidents included in the list of types of operational reliability incidents.

List of types of incidents agreed with the federal executive authority liable for ensuring security, other than cases of unlawful disclosure of bank secret and (or) protected information under regulatory acts of the Bank of Russia, and list of types of operational reliability incidents broken down by activities of credit institutions, non-banking financial institutions and national payment system subjects and their constituent technological processes (hereinafter, the list of types of information security and operational reliability incidents) are set forth in [Appendix 11](#_bookmark31) hereto.

* 1. PROVISION BY INFORMATION EXCHANGE PARTICIPANTS OF DATA ABOUT IDENTIFICATION OF AN INFORMATION SECURITY INCIDENT

Data about identification of an information security incident shall be sent by information exchange participants to the Bank of Russia under paragraph eight, clause 8 of Regulation No. 683-P of the Bank of Russia [5], paragraph two, clause 1.15 of Regulation No. 757-P of the Bank of Russia [7] and paragraph two, clause 1.5 of Regulation No. 719-P of the Bank of Russia [6] upon identification of criteria of notification of an information security incident in accordance with the list of types of information security incidents set forth in section 6.1.

Upon identification of the specified notification criteria information exchange participants send data about identification of an information security incident within the below time frames, unless otherwise required by the regulatory acts of the Bank of Russia:

* + - within 3 hours from the moment of identification of an information security incident for information exchange participants using an enhanced or standard information security level under GOST R 57580.1-2017 [12];
    - within 24 hours from the moment of identification of an information security incident for any other information exchange participants.

Form of provision by information exchange participants of data about identification of an information security incident (*NTF\_ISI\_Detect*) to the Bank of Russia is set forth in [Appendix 12](#_bookmark32) hereto.

* 1. PROVISION BY INFORMATION EXCHANGE PARTICIPANTS OF DATA ABOUT IDENTIFICATION OF UNLAWFUL DISCLOSURE OF BANK SECRET AND (OR)

PROTECTED INFORMATION UNDER REGULATORY ACTS OF THE BANK OF RUSSIA

Data about identification of unlawful disclosure of bank secret and (or) protected information under regulatory acts of the Bank of Russia shall be sent by information exchange participants to the Bank of Russia upon identification by an information exchange participant of the fact of unlawful disclosure of bank secret and (or) protected information under paragraph two, clause 1.15 of Regulation No. 757-P of the Bank of Russia [7], paragraphs one and eight, clause 8 of Regulation No. 683-P of the Bank of Russia [5] subject to the provisions of clauses 7.3 and 7.6 of Bank of Russia Regulation No. 716-P, dated 8 April 2020, ‘On Requirements to the Operational Risk Management System in a Credit Institution and Banking Group’ (hereinafter, Regulation No. 716-P of the Bank of Russia) [11], paragraph two, clause 1.5 of Regulation No. 719-P of the Bank of Russia [6], provided that information about the fact of unlawful disclosure of personal data have not been previously sent to the Bank of Russia in terms of cooperation between information exchange participants and the Bank of Russia upon identification of computer incidents as well as in cases provided for by section 6.5. hereof.

Upon identification of the specified criterion of sending a data provision form information exchange participants shall send data about identification of unlawful disclosure of bank secret and (or) protected information within the below time frames, unless otherwise required by the regulatory acts of the Bank of Russia:

* + - within 3 hours from the moment of identification of an information security incident for information exchange participants using an enhanced or standard information security level under GOST R 57580.1-2017 [12];
    - within 24 hours from the moment of identification of an information security incident for any other information exchange participants.

Form of provision by information exchange participants of data about identification of unlawful disclosure of bank secret and (or) protected information under regulatory acts of the Bank of Russia (*NTF\_ISI\_DataLeak*) is set forth in [Appendix 13](#_bookmark33) hereto.

* 1. PROVISION BY INFORMATION EXCHANGE PARTICIPANTS OF DATA ABOUT THE FINDINGS OF INVESTIGATION OF AN INFORMATION SECURITY INCIDENT OR UNLAWFUL DISCLOSURE OF BANK SECRET AND (OR) PROTECTED

INFORMATION UNDER REGULATORY ACTS OF THE BANK OF RUSSIA

Data about the findings of investigation of an information security incident or unlawful disclosure of bank secret and (or) protected information under regulatory acts of the Bank of Russia shall be sent by information exchange participants to the Bank of Russia under paragraph two, clause 1.15 of Regulation No. 757-P of the Bank of Russia [7], paragraphs

one and eight, clause 8 of Regulation No. 683-P of the Bank of Russia [5] subject to the provisions of clauses 7.3 and 7.6 of Regulation No. 716-P of the Bank of Russia [11], where an information exchange participant has previously submitted to the Bank of Russia the form for provision of data about identification of an information security incident or unlawful disclosure of bank secret and (or) protected information under regulatory acts of the Bank of Russia.

Upon identification of the specified criterion of sending a data provision form information exchange participants shall send data about the findings of investigation of an information security incident or unlawful disclosure of bank secret and (or) protected information under regulatory acts of the Bank of Russia within 30 days from the moment of sending to the Bank of Russia of the form for provision of data about identification of an information security incident or unlawful disclosure of bank secret and (or) protected information, unless otherwise required by the regulatory acts of the Bank of Russia.

Form of provision by information exchange participants of data about the findings of investigation of an information security incident or unlawful disclosure of bank secret and (or) protected information under regulatory acts of the Bank of Russia (*NTF\_ ISI\_Investigation*) to the Bank of Russia is set forth in [Appendix 14](#_bookmark34) hereto.

* 1. REQUEST OF THE BANK OF RUSSIA FOR THE PURPOSES OF ACKNOWLEDGING THE FACT OF UNLAWFUL DISCLOSURE OF BANK SECRET AND (OR) PROTECTED INFORMATION

UNDER REGULATORY ACTS OF THE BANK OF RUSSIA

Request of the Bank of Russia to an information exchange participant shall be sent by the Bank of Russia under the legislation of the Russian Federation (in particular, paragraphs one and eight, clause 8 of Regulation No. 683-P of the Bank of Russia [5] subject to the provisions of clauses 7.3 and 7.6 of Regulation No. 716-P of the Bank of Russia [11] upon identification of the fact of unlawful disclosure of bank secret and (or) protected information under regulatory acts of the Bank of Russia for the purposes of acknowledging the fact of unlawful disclosure of bank secret and (or) protected information under regulatory acts of the Bank of Russia.

Upon receipt of the request for the purposes of acknowledging the fact of unlawful disclosure of bank secret and (or) protected information under regulatory acts of the Bank of Russia information exchange participants shall send the below data provision forms within the specified time frames:

* data provision form *NTF\_ISI\_DataLeak* within 24 hours, where the fact of unlawful disclosure of bank secret and (or) protected information under regulatory acts of the Bank of Russia is identified based on the information from the Bank of Russia's request;
* form *RESP\_ISI\_DataLeak* within 24 hours, where no fact of unlawful disclosure of bank secret and (or) protected information under regulatory acts of the Bank of Russia has been identified based on the information from the Bank of Russia's request.

Form of the Bank of Russia's request sent to an information exchange participant for the purposes of acknowledging the fact of unlawful disclosure of bank secret and (or) protected information under regulatory acts of the Bank of Russia (*REQ\_ISI\_DataLeak*), as well as form of submission of a response to the Bank of Russia containing information about non-identification of the fact of unlawful disclosure of bank secret and (or) protected information under regulatory acts of the Bank of Russia (*RESP\_ISI\_DataLeak*), sent in cases provided for by paragraph 4, section 6.5 hereof, are set forth in [Appendix 15](#_bookmark35) hereto.

* 1. PROVISION BY INFORMATION EXCHANGE PARTICIPANTS OF DATA ABOUT IDENTIFICATION OF AN OPERATIONAL RELIABILITY INCIDENT

Data about identification of an operational reliability incident shall be sent by information exchange participants to the Bank of Russia under paragraph two, clause 11 of Regulation No. 787-P of the Bank of Russia [9] and paragraph two, clause 1.15 of Regulation No. 779-P of the Bank of Russia [10] upon identification of criteria of notification about information security incidents as set forth in section 6.1.

Upon identification of the specified notification criteria information exchange participants send data about identification of an operational reliability incident within the below time frames, unless otherwise required by the regulatory acts of the Bank of Russia:

* + - within 3 hours from the moment of identification of an operational reliability incident for information exchange participants using an enhanced or standard information security level under GOST R 57580.1-2017 [12];
    - within 24 hours from the moment of identification of an operational reliability incident for any other information exchange participants.

Form of provision by information exchange participants of data about identification of an operational reliability incident (*NTF\_ORI\_Detect*) to the Bank of Russia is set forth in [Appendix 16](#_bookmark36) hereto.

* 1. PROVISION BY INFORMATION EXCHANGE PARTICIPANTS OF DATA ABOUT THE FINDINGS OF INVESTIGATION OF AN OPERATIONAL RELIABILITY INCIDENT

Data about the findings of investigation of an operational reliability incident shall be sent by information exchange participants to the Bank of Russia under paragraph two, clause 11 of Regulation No. 787-P of the Bank of Russia [9] and paragraph two, clause 1.15 of Regulation No. 779-P of the Bank of Russia [10], where an information exchange participant has previously submitted to the Bank of Russia the form for provision of data about identification of an operational reliability incident.

Upon identification of the specified criterion of sending a data provision form information exchange participants shall send data about the findings of investigation of an operational reliability incident within 30 days from the moment of sending to the Bank of Russia of the form for provision of data about identification of an operational reliability incident, unless otherwise required by the regulatory acts of the Bank of Russia.

Form of provision by information exchange participants of data about the findings of investigation of an operational reliability incident (*NTF\_ORI\_Investigation*) to the Bank of Russia is set forth in [Appendix 17](#_bookmark37) hereto.

Scheme of cooperation between the Bank of Russia and information exchange participants upon identification of information security and operational reliability incidents.

Scheme of cooperation between the Bank of Russia and information exchange participants upon identification of information security and operational reliability incidents is shown on Fig. 4.

FIG. 4. SCHEME OF COOPERATION BETWEEN THE BANK OF RUSSIA AND INFORMATION EXCHANGE PARTICIPANTS UPON IDENTIFICATION OF INFORMATION SECURITY AND OPERATIONAL RELIABILITY INCIDENTS



## COOPERATION BETWEEN INFORMATION EXCHANGE PARTICIPANTS AND THE BANK

OF RUSSIA UPON IDENTIFICATION OF COMPUTER INCIDENTS, COMPUTER ATTACKS AND INFORMATION SECURITY VULNERABILITIES

* 1. LIST OF COMPUTER INCIDENTS AND COMPUTER ATTACKS

List of computer incidents and computer attacks including criteria of notification about computer incidents and computer attacks in accordance with requirements of Federal Law No. 187-FZ [2], as well as parts 4, 6 and 7 of Article 27 of Federal Law No. 161-FZ [3], paragraph eight, clause 8 of Regulation No. 683-P of the Bank of Russia [5], paragraph two, clause 1.15 of Regulation No. 757-P of the Bank of Russia [7] and paragraph two, clause 1.15 of Regulation No. 719-P of the Bank of Russia [6] is set forth in [Appendix 18](#_bookmark38) hereto.

* 1. PROVISION BY INFORMATION EXCHANGE PARTICIPANTS OF DATA ABOUT COMPUTER INCIDENTS

Data about computer incidents are sent by information exchange participants to the Bank of Russia in accordance with part 2 of Article 9 of Federal Law No. 187-FZ [2], clause 5 of the Procedure for notification of the Federal Security Service of Russia of computer incidents, response to them, measures to eliminate the consequences of computer attacks taken in respect of significant facilities of critical information infrastructure of the Russian Federation approved by Order No. 282 of the Federal Security Service of Russia, dated 19 June 2019 (hereinafter, the Procedure approved by Order No. 282 of the FSS of Russia), paragraph eight of clause 8 of Regulation No. 683-P of the Bank of Russia [5], paragraph two, clause 1.15 of Regulation No. 757-P of the Bank of Russia [7] and paragraph two, clause 1.5 of Regulation No. 719-P of the Bank of Russia [6] upon identification of criteria of notification about a computer incident in accordance with the list of computer incidents set forth in section 7.1, as well as in cases provided for by section 7.5 hereof.

Upon identification of the specified notification criteria information exchange participants send data about a computer incident within the below time frames:

* + - within 3 hours from the moment of identification of a computer incident due to its relation to the operation of a significant facility of critical information infrastructure;
    - within 24 hours from the moment of identification of a computer incident in all other cases.

Form of provision by information exchange participants of information about computer incidents (*NTF\_CI*) is set forth in [Appendix 19](#_bookmark39) hereto.

[Appendix 20](#_bookmark40) contains the below data provision forms which constitute pre-filled versions of form *NTF\_ CI* and targeted at specific types of computer incidents in accordance with the list of computer incidents:

* + - data provision form *NTF\_CI\_DoS*used by information exchange participants for notification of the Bank of Russia about a computer incident - slowed down operation of a resource as a result of DoS (denial of service) attack;
    - data provision form *NTF\_CI\_ApplicationCompromise*used by information exchange participants for notification of the Bank of Russia about a computer incident - successful use of resource vulnerability;
    - data provision form *NTF\_CI\_MalwareInfection*used by information exchange participants for notification of the Bank of Russia about a computer incident - infection with viral software;
    - data provision form *NTF\_CI\_AccountCompromise*used by information exchange participants for notification of the Bank of Russia about a computer incident - compromise of an account;
    - data provision form *NTF\_CI\_PhishingContent*used by information exchange participants for notification of the Bank of Russia about a computer incident - use of a controlled resource for phishing;
    - data provision form *NTF\_CI\_ProhibitedContent*used by information exchange participants for notification of the Bank of Russia about a computer incident - publication on the controlled resource of information prohibited by the legislation of the Russian Federation;
    - data provision form *NTF\_CI\_SocialEngineering*used by information exchange participants for notification of the Bank of Russia about a computer incident - fraudulent acts based on social engineering methods;
    - data provision form *NTF\_CI\_TrafficHijacking*used by information exchange participants for notification of the Bank of Russia about a computer incident - network traffic capture;
    - data provision form *NTF\_CI\_MalwareCommandControl*used by information exchange participants for notification of the Bank of Russia about a computer incident - involvement of a controlled resource as part of viral software infrastructure;
    - data provision form *NTF\_CI\_Spam*used by information exchange participants for notification of the Bank of Russia about a computer incident - spam mailout from a controlled resource;
    - data provision form *NTF\_CI\_UnauthorisedModification*used by information exchange participants for notification of the Bank of Russia about a computer incident - unauthorised modification of information;
    - data provision form *NTF\_CI\_UnauthorisedAccess*used by information exchange participants for notification of the Bank of Russia about a computer incident - unauthorised information disclosure;
    - data provision form *NTF\_CI\_SIM*used by information exchange participants for notification of the Bank of Russia about a computer incident - change (spoofing) of a mobile subscriber identifier (*IMSI*), mobile equipment identifier (*IMEI*) or a SIM-card.
  1. PROVISION BY INFORMATION EXCHANGE PARTICIPANTS OF DATA ABOUT COMPUTER ATTACKS

Data about computer attacks are sent by information exchange participants to the Bank of Russia under part 2, Article 9 of Federal Law No. 187-FZ [2] and parts 4, 6 and 7 of Article 27 of Federal Law No. 161-FZ [3] upon identification of criteria of notification about a computer attack in accordance with the list of computer attacks set forth in section 7.1, as well as in cases provided for by section 7.5 hereof.

The Bank of Russia is notified of computer attacks in the format of an aggregated notification for the reporting period (period for which aggregated data about computer attacks are provided). Aggregated data include aggregation of data related to certain computer attacks of one type, in accordance with the list of computer attacks set forth in section 7.1 in the unified data provision form. Data are aggregated in the fields of the data provision form.

Upon identification of the specified notification criteria information exchange participants send data about computer attacks in the reporting period within the below time frames:

* data about computer attacks in cases, where the malicious activity object constitutes a resource, the IP-address whereof under the register of addressed and numbered resources

belongs to the Russian Federation, are aggregated for three calendar days and sent within 3 calendar days following the reporting period;

* data about computer attacks in cases, where the malicious activity object constitutes another resource, are aggregated for 7 calendar days and sent within 7 calendar days following the reporting period;
* data about computer attacks for another period shall be aggregated as agreed with FinTsERT of the Bank of Russia.

Form of provision by information exchange participants of information about computer attacks (*NTF\_CA*) is set forth in [Appendix 21](#_bookmark53) hereto.

[Appendix 22](#_bookmark54) contains the below data provision forms which constitute pre-filled versions of form *NTF\_CA* and targeted at specific types of computer attacks in accordance with the list of computer attacks:

* data provision form *NTF\_CA\_DoS*used by information exchange participants for notification of the Bank of Russia about DoS (denial of service) attacks;
* data provision form *NTF\_CA\_ExploitAttempt*used by information exchange participants for notification of the Bank of Russia about computer attacks - attempted use of vulnerabilities;
* data provision form *NTF\_CA\_InfectionAttempt*used by information exchange participants for notification of the Bank of Russia about computer attacks - attempted deployment of malware modules;
* data provision form *NTF\_CA\_LoginAttempt*used by information exchange participants for notification of the Bank of Russia about computer attacks - failed authorisation attempts;
* data provision form *NTF\_CA\_Phishing*used by information exchange participants for notification of the Bank of Russia about computer attacks - detection of phishing mailouts or resources;
* data provision form *NTF\_CA\_SocialEngineering*used by information exchange participants for notification of the Bank of Russia about computer attacks - fraudulent acts based on social engineering methods;
* data provision form *NTF\_CA\_Scanning*used by information exchange participants for notification of the Bank of Russia about computer attacks - network scanning of a controlled resource.
  1. PROVISION BY INFORMATION EXCHANGE PARTICIPANTS OF DATA ABOUT IDENTIFIED INFORMATION SECURITY VULNERABILITIES

Data about identified information security vulnerabilities are sent by information exchange participants to the Bank of Russia under part 2 of Article 9 of Federal Law No. 187-FZ [2], as well as Regulations of the Bank of Russia No. 757-P [7], No. 683-P [5], No. 719-P [6] upon detection as a result procedures performed to control absence of any known (described) information security vulnerabilities or regular testing of information infrastructure facilities for penetrations and analysis of information security vulnerabilities of information infrastructure facilities, as provided for by Regulations of the Bank of Russia No. 683-P [5], No. 719-P [6], No. 757-P [7], of information security vulnerabilities of information infrastructure facilities obtained from a third-party supplier organisation under a license or supply agreement, and information about such information security vulnerability is not placed on the official website of the supplier organisation or in applied software distributed by an information exchange participant among third-party organisations, as well as in cases provided for by section 7.5 hereof.

Upon identification of the specified notification criteria information exchange participants send data about information security vulnerabilities within the below time frames:

* + - within 24 hours from the moment of unaided identification of an information security vulnerability;
    - within 3 days from the moment of receipt of a third-party organisation's report containing information about information security vulnerabilities of information infrastructure facilities.

Form of provision by information exchange participants of information about identified information security vulnerabilities (*NTF\_VLN*) is set forth in [Appendix 23](#_bookmark62) hereto.

* 1. REQUEST OF THE BANK OF RUSSIA FOR THE PURPOSES OF RECEIVING INFORMATION OF AN IDENTIFIED COMPUTER ATTACK OR AN INFORMATION SECURITY VULNERABILITY

Request to an information exchange participant for the purposes of receiving information of an identified computer attack or an information security vulnerability, where necessary, is sent by the Bank of Russia upon receipt of information about a computer attack or an identified information security vulnerability of a computer object of the information exchange participant in order to obtain an acknowledgment of the fact of computer attack or information security vulnerability under part 2 of Article 9 of the Federal Law No. 187-FZ [2], clause 4 of the Procedure approved by Order No. 282 of the FSS of Russia.

Upon receipt of the request for the purposes of receiving information of an identified computer attack or an information security vulnerability information exchange participants shall send the following data provision forms within the specified time frames:

* data provision form *NTF\_CI* within 3 hours in case of identification based on the information from the Bank of Russia's request of a computer incident related to operation of a significant facility of critical information infrastructure;
* data provision form *NTF\_CI* within 24 hours in case of identification based on the information from the Bank of Russia's request of a computer incident not related to operation of a significant facility of critical information infrastructure;
* data provision form *NTF\_CA* within 24 hours in case of identification based on the information from the Bank of Russia's request of a computer attack;
* data provision form *NTF\_VLN* within 24 hours in case of identification based on the information from the Bank of Russia's request of an information security vulnerability of a computer object;
* form *RESP\_IEP\_Detect* within 24 hours in case base don the information from the Bank of Russia's request no computer incidents, computer attacks or information security vulnerabilities have been identified.

Form of the Bank of Russia's request sent to an information exchange participant for the purposes of receiving information of an identified computer attack or an information security vulnerability (*REQ\_IEP\_Detect*), as well as form of submission of response to the Bank of Russia containing information about non-identification of a computer attack or an information security vulnerability (*RESP\_IEP\_Detect*) sent in cases provided for by paragraph 7, section 7.5 hereof, are set forth in [Appendix 24](#_bookmark63) hereto.

* 1. REQUEST OF THE BANK OF RUSSIA FOR THE PURPOSES OF RECEIVING DATA ABOUT AN INFORMATION EXCHANGE PARTICIPANT'S OWNERSHIP OF AN INTERNET RESOURCE

The Bank of Russia's request to an information exchange participant for the purposes of receiving data about its ownership of an Internet resource shall be sent by the Bank of Russia upon receipt of the information about an Internet resource containing a malicious code,

phishing information or information prohibited by the Russian legislation, in terms of notification about computer incidents or attacks in order to obtain an acknowledgment of an information exchange participant's ownership of the identified Internet resource for the Bank of Russia's implementation of the provisions of Article 6.2 of Federal Law No. 86-FZ [1].

Upon receipt of a request for the purposes of receiving data about ownership of the identified Internet resource information exchange participants shall send information within 24 hours from the moment of receipt of the Bank of Russia's request.

Form of the Bank of Russia's request sent to an information exchange participant for the purposes of receiving information of an information exchange participant's ownership of the Internet resource(*REQ\_IEP\_Detect*), as well as form of submission of response to the Bank of Russia containing information of an information exchange participant's ownership of the Internet resource(*RESP\_IEP\_Detect*) are set forth in [Appendix 25](#_bookmark64) hereto.

* 1. SCHEME OF COOPERATION BETWEEN THE BANK OF RUSSIA AND INFORMATION EXCHANGE PARTICIPANTS UPON IDENTIFICATION OF COMPUTER INCIDENTS, COMPUTER ATTACKS

AND INFORMATION SECURITY VULNERABILITIES

Scheme of cooperation between the Bank of Russia and information exchange participants upon identification of computer incidents, computer attacks and information security vulnerabilities is shown on Fig. 5.

FIG. 5. SCHEME OF COOPERATION BETWEEN THE BANK OF RUSSIA AND INFORMATION EXCHANGE PARTICIPANTS UPON IDENTIFICATION OF COMPUTER INCIDENTS, COMPUTER ATTACKS AND INFORMATION SECURITY VULNERABILITIES



## COOPERATION BETWEEN INFORMATION EXCHANGE PARTICIPANTS AND THE BANK OF RUSSIA FOR THE PURPOSES OF SUSPENSION/RESUMPTION OF

E-MESSAGE EXCHANGE UPON IDENTIFICATION OF INFORMATION SECURITY INCIDENTS DURING FUNDS

TRANSFERS USING ENTS AT INFORMATION INFRASTRUCTURE FACILITIES OF INFORMATION EXCHANGE PARTICIPANTS

Request to the Bank of Russia about suspension/resumption of e-message exchange shall be sent to information exchange participants - ENTS participants to the Bank of Russia under clause 19 of Bank of Russia Regulation No. 802-P, dated 25 July 2022, ‘On Requirements for Protection of Information Within the Payment System of the Bank of Russia’ (hereinafter, Regulation No. 802-P of the Bank of Russia) [8] upon identification of information security incidents during funds transfers using ENTS at information infrastructure facilities of information exchange participants which have resulted or may result in a funds transfer without consent of the information exchange participant.

Upon identification of the specified notification criteria information exchange participants send data about suspension/resumption of e-message exchange under clause 18 of Regulation No. 802-P of the Bank of Russia. Form of request of an information exchange participant using ENTS for funds transfers sent to the Bank of Russia for the purposes of suspension/resumption of e-message exchange upon identification of information security incidents during funds transfers using ENTS at information infrastructure facilities of information exchange participants (*REQ\_ IEP\_CorrAccLock*), is set forth in [Appendix 26](#_bookmark65) hereto.

Upon receipt of the request from the information exchange participant the Bank of Russia sends a notification of consideration of request under clause 19.5 of Regulation No. 802-P of the Bank of Russia [8]. Form for submission of response to an information exchange participant containing information about consideration of the request of suspension/resumption of e-message exchange (*RESP\_IEP\_CorrAccLock*), is set forth in [Appendix 26](#_bookmark65) hereto.

Scheme of cooperation between the Bank of Russia and information exchange participants upon request for suspension/resumption of e-message exchange upon identification of information security incidents during funds transfers using ENTS at information infrastructure facilities of information exchange participants is shown on Fig. 6.

FIG. 6. SCHEME OF COOPERATION BETWEEN THE BANK OF RUSSIA AND INFORMATION EXCHANGE PARTICIPANTS UPON REQUEST FOR SUSPENSION/RESUMPTION OF E-MESSAGE EXCHANGE UPON IDENTIFICATION OF INFORMATION SECURITY INCIDENTS DURING FUNDS TRANSFERS AT INFORMATION INFRASTRUCTURE FACILITIES OF INFORMATION EXCHANGE PARTICIPANTS



## SENDING BY INFORMATION EXCHANGE PARTICIPANTS TO THE BANK OF RUSSIA OF INFORMATION ABOUT THE PLANNED MEASURES TO DISCLOSE INFORMATION ABOUT IDENTIFIED INFORMATION SECURITY AND OPERATIONAL

RELIABILITY INCIDENTS

Data about the planned measures to disclose information about identified information security or operational reliability incidents shall be sent by information exchange participants to the Bank of Russia under paragraph four of clause 1.15 of Regulation No. 757-P of the Bank of Russia [7], paragraph nine of clause 8 of Regulation No. 683-P of the Bank of Russia [5], paragraph three of clause 1.5 of Regulation No. 719-P of the Bank of Russia [6], paragraph three of clause 11 of Regulation No. 787-P of the Bank of Russia [9] and paragraph three of clause 1.15 of Regulation No. 779-P of the Bank of Russia [10], upon occurrence of the below condition: an information exchange participant plans measures including production of press releases and holding press conferences, placement of information on the official websites on the Internet in respect of information security or operational reliability incidents.

Upon identification of the specified notification criteria information exchange participants send data about the planned measures to disclose information about identified information security or operational reliability incidents within the time frames established by paragraph four of clause 1.15 of Regulation No. 757-P of the Bank of Russia [7], paragraph nine of clause 8 of Regulation No. 683-P of the Bank of Russia [5], paragraph three of clause 1.5 of Regulation No. 719-P of the Bank of Russia [6], paragraph three of clause 11 of Regulation No. 787-P of the Bank of Russia [9] and paragraph three of clause 1.15 of Regulation No. 779-P of the Bank of Russia [10].

Form of submission by information exchange participants to the Bank of Russia of information of the planned measures to disclose information about identified information security or operational reliability incidents (*NTF\_IEP\_Publication*), is set forth in [Appendix 27](#_bookmark66) hereto.

Scheme of cooperation between the Bank of Russia and information exchange participants upon submission of information of the planned measures to disclose information about identified information security or operational reliability incidents is shown on Fig. 7.

FIG. 7. SCHEME OF COOPERATION BETWEEN THE BANK OF RUSSIA AND INFORMATION EXCHANGE PARTICIPANTS UPON SUBMISSION OF INFORMATION OF THE PLANNED MEASURES TO DISCLOSE INFORMATION ABOUT IDENTIFIED INFORMATION SECURITY OR OPERATIONAL RELIABILITY INCIDENTS



## APPENDICES

APPENDIX 1. DATA PROVISION FORM NTF\_OWC\_SNPS – FORM OF PROVISION OF DATA BY INFORMATION EXCHANGE PARTICIPANTS -

FUNDS TRANSFER OPERATORS, PAYMENT SYSTEM

OPERATORS, PAYMENT INFRASTRUCTURE SERVICE PROVIDERS ABOUT ALL CASES AND (OR) ATTEMPTS OF FUNDS TRANSFERS WITHOUT THE

CLIENT'S CONSENT

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 1 | Type of notification | Type of notification | O | - | [NTF\_OWC\_SNPS] | Pre-filled field |
| 2 | Information  about payer's identifiers (identifying the payer) | INN (Taxpayer Identification Number) | CO | If the payer is a legal entity, otherwise, if any | In accordance with the format of the Federal Tax Service of Russia | At least one of the fields must be filled in |
| 3 | The result of calculation of the special code of ID number | CO | If the payer is an individual | The result of calculation of hash function SHA-256 |
| 4 | The result of calculation of the special code of SNILS number | CO | If the payer is an individual, if any | The result of calculation of hash function SHA-256 | - |
| 5 | Mobile telephone communications subscriber's number | CO | If the payer is an individual, otherwise, if any | In accordance  with the international numbering system and plan | Mobile telephone communications subscriber's number of the payer acknowledged under cl. 5.2.1 of Regulation No. 683-P |
| 6 | Criteria of legitimacy of operation without consent characterising the payer | Criteria of legitimacy of operation without consent characterising the payer | CO | If the payer meets at least one of legitimacy criteria | From the classifier  "Criteria of operation legitimacy (signs of funds transfer without consent of the client) without consent" set forth  in [Appendix 28](#_bookmark67) | All criteria of legitimacy of operation without consent characterising the payer shall be chosen |
| 7 | Information  about the payer's payment facility | Type of payer's payment facility | O | - | Selection of one value from the list: [Cash] [Bank account] [Payment card] [Mobile telephone communications subscriber's number] [E-wallet] | - |
| 8 | Bank account number | CO | Field "Type of payment facility" = [Bank account] | In accordance  with the format determined in Regulation of the Bank of Russia  No. 579-P | - |
| 9 | BIC of funds  to transfer funds | In accordance  with the format determined in Regulation of the Bank of Russia  No. 732-P | - |
| 10 | Number of payment card | CO | Field "Type of payment facility" = [Payment card] | In accordance with the format ISO/IEC 7812 | - |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 11 |  | Mobile telephone communications subscriber's number | CO | Field "Type of payment facility" = [Mobile telephone communications subscriber's number] | In accordance  with the international numbering system and plan | - |
| 12 | E-wallet identifier | CO | Field "Type of payment facility" = [E-wallet] | In accordance with the format of e-wallets identifiers determined by electronic funds operator | - |
| 13 | INN of electronic funds operator having issued an e-wallet | In accordance with the format approved by the Federal Tax Service of Russia |  |
| 14 | Information about operation method | Technology of funds transfer | O | - | Selection of one value from the list:  [INT]  [CARD] [WALLET] [PS BR]  [SPFS] [SWIFT] [SBP] [MONEY]  The list depends  on the field "Type of payer's payment facility" | [INT] – internal transfer  [CARD] - card payment systems [WALLET] - payment systems without account opening [PS\_BR] - inter-bank transfers using the Payment System of te Bank of Russia  [SPFS] - inter-bank transfers using FMS (Financial Messaging System)  [SWIFT] - inter-bank transfers using SWIFT  [SBP] - inter-bank transfers using FPS [MONEY] - faster payments  without account opening |
| 15 | Payment system | CO | Field "Technology of funds transfer" = [CARD], [WALLET], [MONEY] | INN, in accordance with the format of the Federal Tax Service of Russia, or [Other] | In case of availability of INN for a payment system operator or electronic funds operator, INN is to be specified, otherwise [Other] |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 16 |  | Type of operation | O | - | "Selection of one value from the list: [FUND]  [WITHDRAW] [TRANSFER] [CROSS] [PURCHASE] [CHARGEBACK] [B2B]  [B2C]  [C2B]  [C2C]  [C2G]  The list depends on the fields "Type of payer's payment facility"  and "Payment system" | [FUND] - depositing cash funds  [WITHDRAW] - withdrawal of funds  [TRANSFER] –  transfer of funds between homogeneous payment facilities  [CROSS] - funds transfer involving conversion  between different-type payment facilities [PURCHASE] -  purchase  [CHARGEBACK] -  chargeback  [B2B] – B2B - FPS operations  [B2C] – B2C - FPS operations  [C2B] – C2B - FPS operations  [C2C] – C2C - FPS operations  [C2G] – C2G -  FPS operations |
| 17 | Information  about recipient's payment facility | Type of funds recipient's payment facility | CO | Field "Type of operation"  = [PURCHASE], [C2B],  [B2B] is filled in,  in case of availability of | "Selection of one value from the list: [Cash] [Bank account] | - |
|  |  |  |  |  | [Payment card] |  |
|  |  |  |  |  | [Mobile telephone |  |
|  |  |  |  |  | communications |  |
|  |  |  |  |  | subscriber's number] |  |
|  |  |  |  |  | [E- |  |
|  |  |  |  |  | wallet] |  |
|  |  |  |  |  | The list depends |  |
|  |  |  |  |  | on the fields "Payment |  |
|  |  |  |  |  | system" and "Type of |  |
|  |  |  |  |  | operation" |  |
| 18 |  | Bank account number | CO | Field "Type of payment facility" = [Bank account] | In accordance  with the format determined  in Regulation No. 579-P of the Bank of Russia | - |
|  |  |  |  |  |
|  |  |  |  |  |
| 19 |  | BIC of funds |  | In accordance  with the format determined  by Regulation of the Bank of Russia  No. 732-P | - |
|  |  | transfer |  |  |
|  |  | operator |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| 20 |  | Number of payment card | CO | Field "Type of payment facility" = [Payment card] | In accordance with the format ISO/IEC 7812 | - |
| 21 |  | Mobile telephone | CO | Field "Type of  payment facility" =  [Mobile telephone  communications  subscriber's number] | In accordance  with the international  numbering system  and plan | - |
|  |  | communications |  |  |
|  |  | subscriber's number |  |  |
|  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 22 |  | E-wallet identifier | CO | Field "Type of payment facility" = [E-wallet] | In accordance with the format of e-wallets identifiers determined by electronic funds operator | - |
| 23 | INN of electronic funds operator having issued an e-wallet | In accordance with the format approved by the Federal Tax Service of Russia | - |
| 24 | Information  about funds recipient's identifiers (identifying the recipient of funds) | INN (Taxpayer Identification Number) | CO | Field "Technology of funds transfer" = [INT] | In accordance with the format of the Federal Tax Service of Russia | At least one of the fields must be filled in |
| 25 | The result of calculation of the special code of ID number | The result of calculation of hash function SHA-256 |
| 26 | The result of calculation of the special code of SNILS number | The result of calculation of hash function SHA-256 | In case of availability of |
| 27 | Mobile telephone communications subscriber's number | In accordance  with the international numbering system and plan | Mobile telephone communications subscriber's number of the funds recipient acknowledged  in accordance  with cl. 5.2.1 of the Regulation  No. 683-P |
| 28 | Criteria of legitimacy of operation without consent characterising the funds recipient | Criteria of legitimacy of operation without consent characterising the funds recipient | CO | Field "Technology of funds transfer" = [INT],  and the funds recipient meets at least one of legitimacy criteria | From the classifier  "Criteria of operation legitimacy (signs of funds transfer without consent of the client) without consent" set forth  in [Appendix 28](#_bookmark67) | All criteria of legitimacy of operation without consent characterising the funds recipient shall be chosen |
| 29 | Information determining the funds transfer operation | Date and time of operation | O | - | In accordance with RFC 3339 | Moscow time [UTC +03:00] |
| 30 | Amount of operation | O | - | Amount net of bank fees  accurate to two  decimal places | - |
| 31 | Operation currency | O | - | From the All-Russian currency classifier | - |
| 32 | Amount of operation  in rubles at the internal  exchange rate | CO | Field "Operation currency" ≠ [RUB] | Amount accurate to two decimal places | - |
| 33 | Purpose of payment | N | - | Text field | - |
| 34 | BIC of funds transfer operator rendering services to the funds recipient | O | - | In accordance  with the format determined in Regulation of the Bank of Russia  No. 732-P | - |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 35 |  | Identifier of funds transfer operator rendering services to the payer, using FMS or SWIFT | CO | Field "Technology of funds transfer" = [SPFS], [SWIFT] | In accordance with SWIFT format | SWIFT-code of the payer |
| 36 | Identifier of funds transfer operator rendering services to the funds recipient, using FMS or SWIFT | In accordance with SWIFT format | SWIFT-code of the funds recipient |
| 37 | SWIFT operation identifier (operation number) | In accordance with SWIFT format | - |
| 38 | Identifier of retail and service outlet | CO | In case of operation  to the benefit of retail and service outlet | In accordance  with the format approved in the payment  system | MerchantID |
| 39 | INN of retail and service outlet | CO | In case of operation  to the benefit of retail and service outlet,  if any | In accordance with the format approved by the Federal Tax Service of Russia | - |
| 40 | Reference number of operation (transaction) | CO | Field "Technology of funds transfer" = [CARD] | In accordance  with the format approved in the payment  system | Retrieval Reference Number (RRN) |
| 41 | Operation (Transaction) response code | [Approved] [Denied] | Response Code |
| 42 | Chargeback reason code | In accordance  with the format approved in the payment  system | Reason Code |
| 43 | BIN of funds transfer operator - acquirer | In accordance  with the format approved in the payment  system | - |
| 44 | Code reflecting the core activity of retail and service outlet | CO | Field "Technology of funds transfer" = [CARD],  and filling-in this field in authorisation messages is provided for  by PS standards | In accordance  with the format approved in the payment system | MCC |
| 45 | Token value upon a tokenised operation | CO | Field "Technology of funds transfer" = [CARD],  and a tokenised card operation  was conducted | In accordance  with the format approved in the payment system | Token Number |
| 46 | FPS identifier of funds transfer operator rendering services to the funds recipient | CO | Field "Technology of funds transfer" = [SBP], | In accordance  with FPS Operations and Payments Clearing Center (OPCC) standards | MemberID |
| 47 | FPS operation identifier (operation number) | CO | Field "Technology of funds transfer" = [SBP], | In accordance  with FPS Operations and Payments Clearing Center (OPCC) standards | TR ID |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 48 |  | Identifier of FPS payment reference | CO | Field "Technology of funds transfer" = [SBP],  and "Type of operation" = [B2B], [C2B], [C2G],  and the operation was conducted using the payment  reference | In accordance  with FPS Operations and Payments Clearing Center (OPCC) standards | QRC\_ID |
| 49 | Information about operation without consent | Condition of notification of an operation without consent | O | - | Selection of one value from the list:  [Client OWC] [Client Attempt] [Participant] [DB]  [IND]  [REQ] | [Client OWC] - client's notification of OWC  [Client Attempt] - client's notification of attempted OWC [Participant] - notification from PS participant  [DB] - availability of OWC DB  [IND] - identifying signs of OD-2525 [REQ] - receipt  of information about committed wrongful  under the Bank of Russia's request and classification of a funds transfer operation as an operation without  client's consent |
| 50 | Identifier  of request(s) of the Bank of Russia for the purposes of receiving data about the operation without consent based on information on any wrongful acts from the federal executive authority in the field of internal affairs | CO | Field "Condition of notification of an operation without consent"  = [REQ] | In accordance  AIPS FinTsERT format.  Where several identifiers are specified, they are to be enumerated using  ";' | Identifier  of request(s) of the Bank of Russia for the purposes of receiving data about the operation without consent based on information on any wrongful acts from the federal executive authority in the field of internal affairs,  whereunder a funds transfer operation was classified as an operation without consent of the client |
| 51 | Date and time of registration of a notification about operation without consent or identification of attempted operation without consent | O | - | In accordance with RFC 3339 | Moscow time [UTC +03:00] |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 52 |  | Criteria of legitimacy of operation without consent characterising the operation | CO | If the operation meets at least one of legitimacy criteria | From the classifier  "Criteria of operation legitimacy (signs of funds transfer without consent of the client) without consent" set forth  in [Appendix 28](#_bookmark67) | All criteria of legitimacy of operation without consent characterising the operation shall be chosen |
| 53 | Amount of damage | O | - | Amount of operation  including bank fees accurate to two decimal  places | Amount of actual client's losses is specified |
| 54 | Use of UBS for client identification | CO | If client was identified using UBS | [Yes] | - |
| 55 | Information used  for device identification | Operation method | O | - | Selection of one value from the list:  [ATM] [BRANCH] [DBO]. [MB]  [DBO]. [WEB]  [DBO]. [TC] [ECOM]  [POS]  [SST] | [ATM] – using an ATM [BRANCH] - in a credit  institution branch [DBO]. [MB] - using mobile bank [DBO]. [WEB] - using  client bank (thin client)  [DBO]. [TC] - using client bank (thick client)  [ECOM] - using e-commerce facilities  [POS] - using a POS-terminal [SST] - using a self-service  terminal |
| 56 | Device identifier | CO | Field "Operation method" = [ATM], [POS] or [SST] | Text field | Unique identifier of the device used to conduct the operation |
| 57 | Unique numerical identifier of device on the Internet | CO | Field "Operation method"  = [DBO]. [MB], [DBO].  [WEB], [DBO]. [TC] | In accordance  with RFC 791 or RFC 2460 format | Device IP-address |
| 58 | Network address of a computer and (or) communication device (router) | N | - | In accordance with IEEE format | Device MAC-address |
| 59 | International subscriber's identifier (individual number of subscriber - natural person) | N | - | In accordance with ITU-T E. 118 format | SIM-card number (ICCID) |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 60 |  | International identifier of user equipment (terminal equipment) of subscriber - natural person | N | - | In accordance with ITU-T E. 212 format | Device IMSI |
| 61 | Device digital footprint | N | - | Device digital footprint obtained in accordance  with recommendations  of the Bank of Russia | - |
| 62 | Phishing URL | N | - | In accordance with RFC 3986 format | To be filled out in case an operation is initiated from a phishing website |
| 63 | Payer's application to law enforcement structures | Application to law enforcement structures | N | - | [Completed] | - |
| 64 | Date of entry into the crime log | CO | "Application to law enforcement structures" = [Completed], at least one of the blocks  is to be filled in | In accordance with RFC 3339 | Moscow time [UTC +03:00] |
| 65 | Sequential number in the crime log | In accordance with the format established by the Ministry of Internal Affairs of Russia | - |
| 66 | Date of institution of criminal case | CO | In accordance with RFC 3339 | Moscow time [UTC +03:00] |
| 67 | Number of criminal case | In accordance with the format established by the Ministry of Internal Affairs of Russia | - |
| 68 | Necessity of FinTsERT involvement | Necessity to involve FinTsERT to investigate the funds withdrawal chain | CO | Where necessary | [Yes] | - |

APPENDIX 2. DATA PROVISION FORM NTF\_OWC\_OEP - FORM

OF PROVISION BY INFORMATION EXCHANGE PARTICIPANTS - ELECTRONIC PLATFORM OPERATORS OF DATA ABOUT ALL CASES AND (OR) ATTEMPTS

OF FUNDS TRANSFERS WITHOUT THE CLIENT'S CONSENT INCLUDING INFORMATION ABOUT NOMINAL ACCOUNT OPERATIONS WITHOUT CONSENT OF THE BENEFICIARY CLIENT

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 1 | Type of notification | Type of notification | O | - | [NTF\_OWC\_OEP] | Pre-filled field |
| 2 | Condition of notification of an operation without consent | Condition of notification of an operation without consent | O | - | Selection of one value from the list:  [Client OWC] [Client Attempt] [DB]  [UAA] | [Client OWC] - client's notification of OWC  [Client Attempt] - client's notification of attempted OWC  [UAA] - identification of unauthorised access to information infrastructure facilities  [DB] - availability in DB  about OWC |
| 3 | Information  about identifiers of beneficiary client | INN (Taxpayer Identification Number) | CO | If the payer is a legal entity, otherwise, if any | In accordance with the format of the Federal Tax Service of Russia | At least one of the fields must be filled in |
| 4 | The result of calculation of the special code of ID number | CO | If the payer is an individual | The result of calculation of hash function SHA-256 |
| 5 | The result of calculation of the special code of SNILS number | CO | If the payer is an individual, if any | The result of calculation of hash function SHA-256 | - |
| 6 | Information  about identifiers of EPO, on whose nominal account an operation without consent of the beneficiary client was conducted | Nominal account number | O | - | In accordance  with the format determined in Regulation of the Bank of Russia  No. 579-P | - |
| 7 | Name of funds transfer operator, with whom a nominal account is opened | CO | One of the fields must be filled in | From the list generated based on the official funds transfer operators reference book | - |
| 8 | BIC of funds transfer operator, with whom a nominal account is opened | In accordance  with the format determined in Regulation of the Bank of Russia  No. 732-P | - |
| 9 | Information  about identifiers of the funds recipient under the nominal account operation conducted without consent of the beneficiary client | Bank account number | O | - | In accordance  with the format determined in Regulation of the Bank of Russia  No. 579-P | - |
| 10 | Name of funds transfer operator, with whom a bank account is opened | CO | One of the fields must be filled in | From the list generated based on the official funds transfer operators reference book | - |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 11 |  | BIC of funds transfer operator, with whom a bank account is opened |  |  | In accordance  with the format determined in Regulation of the Bank of Russia  No. 732-P | - |
| 12 | Information about a nominal account operation conducted without consent of the beneficiary client | Date and time of operation | O | - | In accordance with RFC 3339 | Moscow time [UTC +03:00] |
| 13 | Amount of operation | O | - | Amount net of bank fees  accurate to two  decimal places | - |
| 14 | Operation currency | O | - | From the All-Russian currency classifier | - |
| 15 | Amount of operation  in rubles at the internal  exchange rate | CO | Field "Operation currency" ≠ [RUB] | Amount accurate to two decimal places | - |
| 16 | Information about operation without consent | Date and time of registration of a notification about operation without consent or identification of attempted operation without consent | CO | Field "Condition of notification of an operation without consent" = [Client OWC], [Client Attempt] | In accordance with RFC 3339 | Moscow time [UTC +03:00] |
| 17 | Criteria of legitimacy of operation without consent | O | - | From the classifier  "Criteria of legitimacy of operation without consent" set forth in [Appendix](#_bookmark67)  [28](#_bookmark67) | All criteria of legitimacy characterising the operation without consent or the payer shall be chosen |
| 18 | Amount of damage | O | - | Amount of operation  including bank fees accurate to two decimal  places | Amount of actual client's losses is specified |
| 19 | Unique numerical identifier of device on the Internet | N | - | In accordance  with RFC 791 or RFC 2460 format | Device IP-address |
| 20 | Network address of a computer and (or) communication device (router) | N | - | In accordance with IEEE format | Device MAC-address |
| 21 | International subscriber's identifier (individual number of subscriber - natural person) | N | - | In accordance with ITU-T E. 118 format | SIM-card number (ICCID) |
| 22 | International identifier of user equipment (terminal equipment) of subscriber - natural person | N | - | In accordance with ITU-T E. 212 format | Device IMSI |
| 23 | Device digital footprint | N | - | Device digital footprint obtained in accordance  with recommendations  of the Bank of Russia | - |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 24 | Payer's application to law enforcement structures | Application to law enforcement structures | N | - | [Completed] | - |
| 25 | Date of entry into the crime log | CO | "Application to law enforcement structures" = [Completed] | In accordance with RFC 3339 | Moscow time [UTC +03:00] |
| 26 | Sequential number in the crime log | In accordance with the format established by the Ministry of Internal Affairs of Russia | - |
| 27 | Date of institution of criminal case | In accordance with RFC 3339 | Moscow time [UTC +03:00] |
| 28 | Number of criminal case | In accordance with the format established by the Ministry of Internal Affairs of Russia | - |
| 29 | Necessity of FinTsERT involvement | Necessity to involve FinTsERT to investigate the funds withdrawal chain | CO | Where necessary | [Yes] | - |

APPENDIX 3. DATA PROVISION FORM NTF\_OWC\_OFP - FORM

OF PROVISION BY INFORMATION EXCHANGE PARTICIPANTS - FINANCIAL PLATFORM OPERATORS OF DATA ABOUT ALL CASES AND (OR) ATTEMPTS

TO CARRY OUT OPERATIONS UNDER FINANCIAL TRANSACTIONS, NOT RELYING ON THE FINANCIAL PLATFORM PARTICIPANT'S WILL

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 1 | Type of notification | Type of notification | Type of notification | O | [NTF\_OWC\_OFP] | Pre-filled field |
| 2 | Condition of notification of an operation without the expressed will | Condition of notification of an operation without the expressed will | O | - | Selection of one value from the list: [Participant\_ accWithdrawal] [IND\_accWithdrawal] [Participant\_OWC] [IND\_OWC] | [Participant\_ accWithdrawal] - notification from a financial platform participant of debiting a special account [IND\_accWithdrawal] - unaided identification of debiting a special account [Participant\_OWC] - notification  of a financial platform participant about a transaction without its will [IND\_OWC] - unaided identification of transaction without the expressed will |
| 3 | Information determining consumer's identifiers (identifying the consumer) | INN (Taxpayer Identification Number) | O | In case of LE (legal entity), otherwise, if any | In accordance with the format of the Federal Tax Service of Russia | At least one of the fields must be filled in |
| 4 | The result of calculation of the special code of ID number | In case of NP (natural person) | The result of calculation of hash function SHA-256 |
| 5 | The result of calculation of the special code of SNILS number | In case of NP, if any | The result of calculation of hash function SHA-256 |
| 6 | Data about a special account of FPO (financial platform operator) opened with the credit institution | Special account number | CO | "Condition of notification" = {«Participant\_ accWithdrawal»,  «IND\_accWithdrawal»} | In accordance  with the format determined in Regulation of the Bank of Russia  No. 579-P | - |
| 7 | Name of the credit institution rendering services to the FPO | CO | The field "Special account number" is filled in.  One of the fields must be filled in | From the list generated based on the official funds transfer operators reference book | - |
| 8 | BIC of the credit institution rendering services to the FPO |  | In accordance  with the format determined in Regulation of the Bank of Russia  No. 732-P | - |
| 9 | Information determining the funds recipient's identifiers (identifying the recipient of funds) | INN (Taxpayer Identification Number) | O | - | In accordance with the format of the Federal Tax Service of Russia | - |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 10 |  | Bank account number | O | - | In accordance  with the format determined in Regulation of the Bank of Russia  No. 579-P | - |
| 11 | Name of funds transfer operator | O | - | From the list generated based on the official funds transfer operators reference book | - |
| 12 | BIC of funds  to transfer funds | O | - | In accordance  with the format determined in Regulation of the Bank of Russia  No. 732-P | - |
| 13 | Information identifying the operation (financial transaction)  (the block is to be filled in for each operation without the expressed will) | Type of financial transaction | CO | "Condition of notification" = {«Participant\_ OWC»,  «IND\_OWC»} | Selection of one value from the list:  [Bank]  [SIB]  [PCB]  [FI]  [Other] | [Bank] - a transaction  to provide financial services [SIB] - a transaction  to provide insurance services [PCB] - a transaction  to provide securities market services  [FI] - a transaction involving financial instruments  [Other] - a transaction  to provide other services of financial nature stipulated by financial platform rules consummated between financial institutions or issuers and financial service consumers  through financial platform, other than bank account (deposit) agreements entered into in view of  entrepreneurial activity carried out by financial service consumer |
| 14 | Date and time of operation | O | - | In accordance with RFC 3339 | Moscow time [UTC +03:00] |
| 15 | Amount of operation | O | - | Amount accurate to two decimal places | - |
| 16 | Operation currency | O | - | From the All-Russian currency classifier | - |
| 17 | Amount of operation  in rubles at the internal  exchange rate | CO | Field "Operation currency" ≠ [RUB] | Amount accurate to two decimal places | - |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 18 | Information about operation without the expressed will  (the block is to be filled in for each operation from the block "Information identifying the operation (financial transaction)" | Date and time of registration of notification about an operation without the expressed will | CO | Field "Condition of notification  of an operation without consent" = [Participant\_ accWithdrawal], [Participant\_OWC] | In accordance with RFC 3339 | Moscow time [UTC +03:00] |
| 19 | Criteria of legitimacy of operation without the expressed will | O | - | From the classifier  "Criteria of legitimacy of operation without consent" set forth in [Appendix](#_bookmark67)  [28](#_bookmark67) | All criteria of legitimacy characterising the operation without the expressed will or the consumer shall be chosen |
| 20 | Amount of damage | O | - | Amount accurate to two decimal places | Amount of actual client's losses is specified |
| 21 | Use of UBS for client identification | CO | If client was identified using UBS | [Yes] | - |
| 22 | Unique numerical identifier of device on the Internet | N | - | In accordance  with RFC 791 or RFC 2460 format | Device IP-address |
| 23 | Network address of a computer and (or) communication device (router) | N | - | In accordance with IEEE format | Device MAC-address |
| 24 | International subscriber's identifier (individual number of subscriber - natural person) | N | - | In accordance with ITU-T E. 118 format | SIM-card number (ICCID) |
| 25 | International identifier of user equipment (terminal equipment) of subscriber - natural person | N | - | In accordance with ITU-T E. 212 format | Device IMSI |
| 26 | Device digital footprint | N | - | Device digital footprint obtained in accordance  with recommendations  of the Bank of Russia | - |
| 27 | Phishing URL | N | - | In accordance with RFC 3986 format | To be filled out in case an operation is initiated from a phishing website |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 28 | Payer's application to law enforcement structures | Application to law enforcement structures | N | - | [Completed] | - |
| 29 | Date of entry into the crime log | CO | "Application to law enforcement structures" = [Completed] | In accordance with RFC 3339 | Moscow time [UTC +03:00] |
| 30 | Sequential number in the crime log | In accordance with the format established by the Ministry of Internal Affairs of Russia | - |
| 31 | Date of institution of criminal case | In accordance with RFC 3339 | Moscow time [UTC +03:00] |
| 32 | Number of criminal case | In accordance with the format established by the Ministry of Internal Affairs of Russia | - |
| 33 | Necessity of FinTsERT involvement | Necessity to involve FinTsERT to investigate the funds withdrawal chain | N | - | [Yes] | - |

APPENDIX 4. DATA PROVISION FORM REQ\_OWC\_IDENTIFICATION -

FORM OF REQUEST OF THE BANK OF RUSSIA FOR THE PURPOSES OF IDENTIFICATION OF RECIPIENT OF FUNDS OR PAYER

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 1 | Type of request/response | Type of request/response | O | - | [REQ\_OWC\_  Identification] | Pre-filled field |
| 2 | Subject of request | Subject of request | O | - | [Funds recipient] [Payer] | - |
| 3 | Information  about the funds recipient's or the payer's payment facility | Type of payment facility | O | - | Selection of one value from the list: [Cash] [Bank account] [Payment card] [Mobile telephone communications subscriber's number] [E-wallet] | - |
| 4 | Bank account number | CO | Field "Type of payment facility" = [Bank account] | In accordance  with the format determined in Regulation of the Bank of Russia  No. 579-P | - |
| 5 | BIC of funds  to transfer funds |  |  | In accordance  with the format determined in Regulation of the Bank of Russia  No. 732-P | - |
| 6 | Number of payment card | CO | Field "Type of payment facility" = [Payment card] | In accordance with the format ISO/IEC 7812 | - |
| 7 | Mobile telephone communications subscriber's number | CO | Field "Type of payment facility" = [Mobile telephone communications subscriber's number] | In accordance  with the international numbering system and plan | - |
| 8 | E-wallet identifier | CO | Field "Type of payment facility" = [E-wallet] | In accordance with the format of e-wallets identifiers determined by electronic funds operator | - |
| 9 | INN of electronic funds operator having issued an e-wallet |  |  | In accordance with the format approved by the Federal Tax Service of Russia | - |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 10 | Information about operation method | Technology of funds transfer | O | - | Selection of one value from the list:  [INT]  [CARD] [WALLET] [PS BR]  [SPFS] [SWIFT] [SBP] [MONEY]  The list depends  on the field "Type of payer's payment facility" | [INT] – internal transfer  [CARD] - card payment systems [WALLET] - payment systems without account opening [PS\_BR] - inter-bank transfers using the Payment System of te Bank of Russia  [SPFS] - inter-bank transfers using FMS (Financial Messaging System)  [SWIFT] - inter-bank transfers using SWIFT  [SBP] - inter-bank transfers using FPS [MONEY] - faster payments  without account opening |
| 11 | Payment system | CO | Field "Technology of funds transfer" = [CARD], [WALLET], [MONEY] | INN, in accordance with the format of the Federal Tax Service of Russia, or [Other] | In case of availability of INN for a payment system operator or electronic funds operator, INN is to be specified, otherwise [Other] |
| 12 | Type of operation | O | - | Selection of one value from the list: [FUND]  [WITHDRAW] [TRANSFER] [CROSS] [PURCHASE] [CHARGEBACK] [B2B]  [B2C]  [C2B]  [C2C]  [C2G]  The list depends on the fields "Type of payer's payment facility"  and "Payment system" | [FUND] - depositing cash funds  [WITHDRAW] - withdrawal of funds  [TRANSFER] –  transfer of funds between homogeneous payment facilities  [CROSS] - funds transfer involving conversion  between different-type payment facilities [PURCHASE] -  purchase  [CHARGEBACK] -  chargeback  [B2B] – B2B - FPS operations  [B2C] – B2C - FPS operations  [C2B] – C2B - FPS operations  [C2C] – C2C - FPS operations  [C2G] – C2G -  FPS operations |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 13 | Information determining the funds transfer operation | Date and time of operation | O | - | In accordance with RFC 3339 | Moscow time [UTC +03:00] |
| 14 | Amount of operation | O | - | Amount net of bank fees  accurate to two  decimal places | - |
| 15 | Operation currency | O | - | From the All-Russian currency classifier | - |
| 16 | Identifier of funds transfer operator rendering services to the payer, using FMS or SWIFT | CO | Field "Technology of funds transfer" = [SPFS], [SWIFT] | In accordance with SWIFT format | SWIFT-code of the payer |
| 17 | Identifier of funds transfer operator rendering services to the funds recipient, using FMS or SWIFT | In accordance with SWIFT format | SWIFT-code of the funds recipient |
| 18 | SWIFT operation identifier (operation number) | In accordance with SWIFT format | - |
| 19 | Identifier of retail and service outlet | CO | In case of operation  to the benefit of retail and service outlet | In accordance  with the format approved in the payment  system | MerchantID |
| 20 | INN of retail and service outlet | CO | In case of operation  to the benefit of retail and service outlet,  if any | In accordance with the format approved by the Federal Tax Service of Russia | - |
| 21 | Reference number of operation (transaction) | CO | Field "Technology of funds transfer" = [CARD] | In accordance  with the format approved in the payment  system | Retrieval Reference Number (RRN) |
| 22 | Operation (Transaction) response code | [Approved] [Denied] | Response Code |
| 23 | Chargeback reason code | In accordance  with the format approved in the payment  system | Reason Code |
| 24 | BIN of funds transfer operator - acquirer | In accordance  with the format approved in the payment  system | - |
| 25 | Code reflecting the core activity of retail and service outlet | CO | Field "Technology of funds transfer" = [CARD],  and filling-in this field in authorisation messages is provided for  by PS standards | In accordance  with the format approved in the payment system | MCC |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 26 |  | Token value upon a tokenised operation | CO | Field "Technology of funds transfer" = [CARD],  and a tokenised card operation  was conducted | In accordance  with the format approved in the payment system | Token Number |
| 27 | FPS identifier of funds transfer operator rendering services to the funds recipient | CO | Field "Technology of funds transfer" = [SBP], | In accordance  with FPS Operations and Payments Clearing Center (OPCC) standards | MemberID |
| 28 | FPS operation identifier (operation number) | CO | Field "Technology of funds transfer" = [SBP], | In accordance  with FPS Operations and Payments Clearing Center (OPCC) standards | TR ID |
| 29 | Identifier of FPS payment reference | CO | Field "Technology of funds transfer" = [SBP],  and "Type of operation" = [B2B], [C2B], [C2G],  and the operation was conducted using the payment  reference | In accordance  with FPS Operations and Payments Clearing Center (OPCC) standards | QRC\_ID |
| 30 | Criteria of legitimacy of operation without consent | Criteria of legitimacy of operation without consent | CO | In case of availability of | From the classifier  "Criteria of operation legitimacy (signs of funds transfer without consent of the client) without consent" set forth  in [Appendix 28](#_bookmark67) | - |
| 31 | Necessity to suspend crediting of funds | Necessity to suspend crediting of funds | CO | Where it is necessary to suspend crediting of funds or to increase the balance of electronic funds of the funds recipient | [Yes] | - |

Data provision form RESP\_OWC\_Identification - Form of submission of response to request of the Bank of Russia for the purposes of identification of recipient of funds or payer

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 1 | Type of request/response | Type of request/response | O | - | [RESP\_OWC\_  Identification] | Pre-filled field |
| 2 | Status | Status | O | - | [Client and operation found]  [Client not found] [Operation not found]  [P2P-operation] [Additional time for consideration is  required] | - |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 3 | Information  about funds recipient's or payer's identifiers | INN (Taxpayer Identification Number) | CO | "Status" = [Client  and operation found] and LE, otherwise, if  any | In accordance with the format of the Federal Tax Service of Russia | At least one of the fields must be filled in |
| 4 | The result of calculation of the special code of ID number | "Status" = [Client  and operation found]  and NP | The result of calculation of hash function SHA-256 |
| 5 | The result of calculation of the special code of SNILS number | "Status" = [Client  and operation found]  and NP, if any | The result of calculation of hash function SHA-256 | In case of availability of |
| 6 | Mobile telephone communications subscriber's number | "Status" = [Client  and operation found] and NP, if any | In accordance  with the international numbering system and plan | Mobile telephone communications subscriber's number of the funds recipient acknowledged  in accordance  with cl. 5.2.1 of the Regulation  No. 683-P |
| 7 | Criteria of legitimacy of operation without consent characterising the funds recipient or the payer | Criteria of legitimacy of operation without consent characterising the funds recipient or the payer | CO | "Status" = [Client  and operation found] and the recipient of funds or the payer meets at least one of legitimacy criteria | From the classifier  "Criteria of operation legitimacy (signs of funds transfer without consent of the client) without consent" set forth  in [Appendix 28](#_bookmark67) | All criteria of legitimacy of operation without consent characterising the funds recipient or the payer shall be chosen |
| 8 | Information about payment facility | Type of payment facility | CO | "Status" = [Client  and operation found] | Selection of one value from the list: [Cash] [Bank account] [Payment card] [Mobile telephone communications subscriber's number] [E-wallet] | - |
| 9 | Bank account number | CO | "Status" = [Client  and operation found], [P2P-operation] and "Type of payment facility" =  [Bank account] | In accordance  with the format determined in Regulation of the Bank of Russia  No. 579-P | - |
| 10 | BIC of funds  to transfer funds |  |  | In accordance  with the format determined in Regulation of the Bank of Russia  No. 732-P | - |
| 11 | Number of payment card | CO | "Status" = [Client  and operation found], [P2P-operation] and "Type of payment facility" =  [Payment card] | In accordance with the format ISO/IEC 7812 | - |
| 12 | Mobile telephone communications subscriber's number | CO | "Status" = [Client  and operation found], [P2P-operation] and "Type of payment facility" = [Mobile telephone communications  subscriber's number] | In accordance  with the international numbering system and plan | - |
| 13 | E-wallet identifier | CO | "Status" = [Client  and operation found], [P2P-operation] and "Type of payment facility"  = [E-wallet] | In accordance with the format of e-wallets identifiers determined by electronic funds operator | - |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 14 |  | INN of electronic funds operator having issued an e-wallet |  |  | In accordance with the format approved by the Federal Tax Service of Russia |  |
| 15 | Information used  for device identification | Operation method | CO | Where information about operation method is available | Selection of one value from the list:  [ATM] [BRANCH] [DBO]. [MB]  [DBO]. [WEB]  [DBO]. [TC] [ECOM]  [POS]  [SST] | [ATM] – using an ATM [BRANCH] - in a credit  institution branch [DBO]. [MB] - using  mobile bank [DBO]. [WEB] -  using  client bank (thin client)  [DBO]. [TC] -  using client bank (thick client)  [ECOM] - using e-commerce facilities  [POS] - using a POS-terminal [SST] - using a self-service  terminal |
| 16 | Device identifier | CO | Field "Operation method" = [ATM], [POS] or [SST] | Text field | Unique identifier of the device used to conduct the operation |
| 17 | Unique numerical identifier of device on the Internet | CO | Field "Operation method"  = [DBO]. [MB], [DBO].  [WEB], [DBO]. [TC] | In accordance  with RFC 791 or RFC 2460 format | Device IP-address |
| 18 | Network address of a computer and (or) communication device (router) | N | - | In accordance with IEEE format | Device MAC-address |
| 19 | International subscriber's identifier (individual number of subscriber - natural person) | N | - | In accordance with ITU-T E. 118 format | SIM-card number (ICCID) |
| 20 | International identifier of user equipment (terminal equipment) of subscriber - natural person | N | - | In accordance with ITU-T E. 212 format | Device IMSI |
| 21 | Device digital footprint | N | - | Device digital footprint obtained in accordance  with recommendations  of the Bank of Russia | - |
| 22 | Suspension of funds crediting | Suspension of funds crediting | CO | REQ\_OWC\_  Identification:  "Necessity to suspend crediting of  funds" = [Yes] | [Suspended] [Suspension impossible] | - |

APPENDIX 5. DATA PROVISION FORM REQ\_OWC\_UUID - FORM OF REQUEST OF THE BANK OF RUSSIA FOR THE PURPOSES OF RECEIVING DATA ABOUT THE OPERATION WITHOUT CONSENT BASED ON INFORMATION ON ANY WRONGFUL

ACTS FROM THE FEDERAL EXECUTIVE AUTHORITY IN THE FIELD OF INTERNAL AFFAIRS

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 1 | Type of request/response | Type of request/response | O | - | [REQ\_OWC\_UUID] | Pre-filled field |
| 2 | Information determining payer's identifiers (identifying the payer) | INN (Taxpayer Identification Number) | O | In case of LE (legal entity), otherwise, if any | In accordance with the format of the Federal Tax Service of Russia | At least one of the fields must be filled in |
| 3 | The result of calculation of the special code of ID number | In case of NP (natural person) | The result of calculation of hash function SHA-256 |
| 4 | The result of calculation of the special code of SNILS number | In case of NP, if any | The result of calculation of hash function SHA-256 |
| 5 | Mobile telephone communications subscriber's number | In case of NP, if any | In accordance  with the international numbering system  and plan |
| 6 | Information about operation method used by the payer | Number of payment card | CO | In case of payer's operation with the payment card | In accordance with the format ISO/IEC 7812 | - |
| 7 | Mobile telephone communications subscriber's number | CO | In case of payer's operation using mobile telephone communications subscriber's number or operation  using  FPS (C2C, C2B, B2C) | In accordance  with the international numbering system and plan | - |
| 8 | Bank account number | CO | In case of payer's operation using bank account or operation  using FPS (B2C, B2B) | In accordance  with the format determined in Regulation of the Bank of Russia  No. 579-P | - |
| 9 | BIC of funds transfer  operator rendering services to  the payer | In accordance  with the format determined in Regulation of the Bank of Russia  No. 732-P | - |
| 10 | E-wallet identifier | CO | In case of payer's operation using e-wallet | In accordance with the format of e-wallets identifiers determined by electronic funds operator | - |
| 11 | Name of electronic funds operator having issued an e-wallet | From the list generated based on the official electronic funds operators reference book | - |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 12 |  | Identifier of ATM or electronic terminal | CO | In case of payer's operation to the retail and service outlet or operation using ATM | In accordance  with the format approved in the payment system | - |
| 13 | Address of ATM or electronic terminal | In accordance  with the structure of FIAS address | - |
| 14 | Name of funds transfer operator servicing the ATM | CO | In case of operation  using ATM | From the list generated based on the official funds transfer operators reference book | - |
| 15 | Information about the method of receiving funds by the recipient | Number of payment card | CO | In case of operation  using recipient's payment card | In accordance with the format ISO/IEC 7812 | To be filled in, where information about the method of receiving funds by the recipient is available |
| 16 | Mobile telephone communications subscriber's number | CO | In case of operation  using a recipient's subscriber's  number | In accordance  with the international numbering system  and plan |
| 17 | Bank account number | CO | In case of operation  using recipient's bank account | In accordance  with the format determined in Regulation of the Bank of Russia  No. 579-P |
| 18 | BIC of funds transfer operator rendering services to the recipient | In accordance  with the format determined in Regulation of the Bank of Russia  No. 732-P |
| 19 | E-wallet identifier | CO | In case of operation  using the recipient's e-wallet | In accordance with the format of e-wallets identifiers determined by electronic funds operator |
| 20 | Name of electronic funds operator having issued an e-wallet | From the list generated based on the official electronic funds operators reference book |
| 21 | INN of retail and service outlet | CO | In case of payer's operation to the retail and service outlet or operation using FPS (C2B, B2B) | In accordance with the format approved by the Federal Tax Service of Russia |
| 22 | Identifier of retail and service outlet | In accordance  with the format approved in the payment  system |
| 23 | Name of funds transfer operator rendering services to the recipient | CO | In case of operation using FPS | From the list generated based on the official funds transfer operators reference book |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 24 | Information identifying the operation | Date and time of operation | O | - | In accordance with RFC 3339 | Moscow time [UTC +03:00] |
| 25 | Amount of operation | O | - | Amount accurate to two decimal places | - |
| 26 | Operation currency | O | - | From the All-Russian currency classifier | - |
| 27 | FPS operation identifier (operation number) | CO | In case of payer's operation using FPS | In accordance  with FPS Operations and Payments Clearing Center (OPCC)  standards | - |
| 28 | BIC of funds transfer operator - acquirer | CO | In case of payer's operation to retail and service outlet | In accordance  with the format determined in Regulation of the Bank of Russia  No. 732-P | - |
| 29 | Reference number of operation (transaction) | CO | In case of payer's operation to retail and service  outlet using  a payment card | In accordance  with the format approved in the payment system | Retrieval Reference Number (RRN) |
| 30 | Identifier of fiscal document | CO | In case of payer's operation to retail and service outlet | In accordance  with requirements of the Federal Law  No. 54-FZ | - |
| 31 | Additional information about operation method | Additional information about operation method | CO | Where the above information is not available | Text field | Textual description of operation method |
| 32 | Information about application  of the client related to funds transfer without consent to the federal executive authority in the field of internal affairs | Date of entry into the crime log | CO | In case of entry into the crime log | In accordance with RFC 3339  Moscow time [UTC +03:00] | One of the paired fields must be filled in |
| 33 | Sequential number in the crime log | In accordance with the format established by the Ministry of Internal Affairs of Russia |
| 34 | Date of institution of criminal case | CO | In case of institution of the criminal case | In accordance with RFC 3339  Moscow  time [UTC +03:00] |
| 35 | Number of criminal case | In accordance with the format established by the Ministry of Internal Affairs of Russia |

Data provision form RESP\_OWC\_UUID - Form of submission of response to request of the Bank of Russia for the purposes of receiving data about the operation without consent based on information on any wrongful acts from the federal executive authority in the field of internal affairs

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 1 | Type of request/response | Type of request/response | O | - | [RESP\_OWC\_UUID] | Pre-filled field |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 2 | Status | Status | O | - | [OWC has already been sent to the Bank of Russia] [Client not found] [Operation not found]  [Additional time for consideration is  required] | - |
| 3 | Identifier of notification of an operation without consent | Identifier of notification of an operation without consent | CO | "Status" = [OWC has been sent to the Bank of Russia] | In accordance  with AIPS FinTsERT format | Identifier of notification of an operation without consent, previously sent to FinTsERT by an information exchange participant |

APPENDIX 6. DATA PROVISION FORM REQ\_OWC\_FORWARD - FORM

OF THE BANK OF RUSSIA'S REQUEST FOR THE PURPOSES OF RECEIVING DATA ABOUT ACTS OF AN INFORMATION EXCHANGE PARTICIPANT RENDERING SERVICES TO THE FUNDS RECIPIENT

TO TRANSFER FUNDS

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 1 | Type of request/response | Type of request/response | O | - | [REQ\_OWC\_Forward] | Pre-filled field |
| 2 | Information  about funds recipient's identifiers (identifying the recipient of funds) | INN (Taxpayer Identification Number) | CO | If the payer is a legal entity, otherwise, if any | In accordance with the format of the Federal Tax Service of Russia | At least one of the fields must be filled in |
| 3 | The result of calculation of the special code of ID number | CO | If the payer is an individual | The result of calculation of hash function SHA-256 |
| 4 | The result of calculation of the special code of SNILS number | CO | If the payer is an individual, if any | The result of calculation of hash function SHA-256 | - |
| 5 | Mobile telephone communications subscriber's number | CO | If the payer is an individual, otherwise, if any | In accordance  with the international numbering system and plan | Mobile telephone communications subscriber's number of the payer acknowledged under cl. 5.2.1 of Regulation No. 683-P |
| 6 | Information  about recipient's payment facility | Type of funds recipient's payment facility | O | - | Selection of one value from the list: [Cash] [Bank account] [Payment card] [Mobile telephone communications subscriber's number] [E-wallet] | - |
| 7 | Bank account number | CO | Field "Type of payment facility" = [Bank account] | In accordance  with the format determined in Regulation of the Bank of Russia  No. 579-P | - |
| 8 | BIC of funds  to transfer funds | In accordance  with the format determined in Regulation of the Bank of Russia  No. 732-P | - |
| 9 | Number of payment card | CO | Field "Type of payment facility" = [Payment card] | In accordance with the format ISO/IEC 7812 | - |
| 10 | Mobile telephone communications subscriber's number | CO | Field "Type of payment facility" = [Mobile telephone communications subscriber's number] | In accordance  with the international numbering system and plan | - |
| 11 | E-wallet identifier | CO | Field "Type of payment facility" = [E-wallet] | In accordance with the format of e-wallets identifiers determined by electronic funds operator | - |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 12 |  | INN of electronic funds operator having issued an e-wallet |  |  | In accordance with the format approved by the Federal Tax Service of Russia | - |
| 13 | Information determining the funds transfer operation | Date and time of operation | O | - | In accordance with RFC 3339 | Moscow time [UTC +03:00] |
| 14 | Amount of operation | O | - | Amount net of bank fees  accurate to two  decimal places | - |
| 15 | Operation currency | O | - | From the All-Russian currency classifier | - |
| 16 | Identifier of funds transfer operator rendering services to the payer, using FMS or SWIFT | CO | Field "Technology of funds transfer" = [SPFS], [SWIFT] | In accordance with SWIFT format | SWIFT-code of the payer |
| 17 | Identifier of funds transfer operator rendering services to the funds recipient, using FMS or SWIFT | In accordance with SWIFT format | SWIFT-code of the funds recipient |
| 18 | SWIFT operation identifier (operation number) | In accordance with SWIFT format | - |
| 19 | Identifier of retail and service outlet | CO | In case of operation  to the benefit of retail and service outlet | In accordance  with the format approved in the payment  system | MerchantID |
| 20 | INN of retail and service outlet | CO | In case of operation  to the benefit of retail and service outlet,  if any | In accordance with the format approved by the Federal Tax Service of Russia | - |
| 21 | Reference number of operation (transaction) | CO | Field "Technology of funds transfer" = [CARD] | In accordance  with the format approved in the payment  system | Retrieval Reference Number (RRN) |
| 22 | Operation (Transaction) response code | [Approved] [Denied] | Response Code |
| 23 | Chargeback reason code | In accordance  with the format approved in the payment  system | Reason Code |
| 24 | BIN of funds transfer operator - acquirer | In accordance  with the format approved in the payment  system | - |
| 25 | Code reflecting the core activity of retail and service outlet | CO | Field "Technology of funds transfer" = [CARD],  and filling-in this field in authorisation messages is provided for  by PS standards | In accordance  with the format approved in the payment system | MCC |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 26 |  | Token value upon a tokenised operation | CO | Field "Technology of funds transfer" = [CARD],  and a tokenised card operation  was conducted | In accordance  with the format approved in the payment system | Token Number |
| 27 | FPS identifier of funds transfer operator rendering services to the funds recipient | CO | Field "Technology of funds transfer" = [SBP], | In accordance  with FPS Operations and Payments Clearing Center (OPCC) standards | MemberID |
| 28 | FPS operation identifier (operation number) | CO | Field "Technology of funds transfer" = [SBP], | In accordance  with FPS Operations and Payments Clearing Center (OPCC) standards | TR ID |
| 29 | Identifier of FPS payment reference | CO | Field "Technology of funds transfer" = [SBP]], "Type of operation' = [B2B], [C2B], [C2G], and operation  was conducted using  a payment reference | In accordance  with FPS Operations and Payments Clearing Center (OPCC) standards | QRC\_ID |
| 30 | Information about analysis of operation without consent | Number of days  before and after the specified operation, for which the funds recipient's operations are to be  analyzed | N | - | Integer number >0 | - |

Data provision form RESP\_OWC\_Forward - Form of submission of response to the Bank of Russia's request for the purposes of receiving data about acts of an information exchange participant rendering services to the funds recipient

to transfer funds

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 1 | Type of request/response | Type of request/response | O | - | [RESP\_OWC\_Forward] | Pre-filled field |
| 2 | Status | Status | O | - | [Client and operation found]  [Client not found] [Operation not found]  [Additional time for consideration is  required] | - |
| 3 | Element underlying the information submitted | Element REQ\_OWC\_ Forward underlying the information submitted | CO | "Status" = [Client  and operation found] | One or the aggregate of values specified  in the request  divided; | - |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 4 | Information about operation method | Technology of funds transfer | CO | "Status" = [Client  and operation found] | Selection of one value from the list:  [INT]  [CARD] [WALLET] [PS BR]  [SPFS] [SWIFT] [SBP] [MONEY]  The list depends  on the field "Type of payer's payment facility" | [INT] – internal transfer  [CARD] - card payment systems [WALLET] - payment systems without account opening [PS\_BR] - inter-bank transfers using the Payment System of te Bank of Russia  [SPFS] - inter-bank transfers using FMS (Financial Messaging System)  [SWIFT] - inter-bank transfers using SWIFT  [SBP] - inter-bank transfers using FPS [MONEY] - faster payments  without account opening |
| 5 | Payment system | CO | Field "Status" = [Client and operation found] and "Technology of funds transfer" = [CARD], [WALLET], [MONEY] | INN, in accordance with the format of the Federal Tax Service of Russia, or [Other] | In case of availability of INN for a payment system operator or electronic funds operator, INN is to be specified, otherwise [Other] |
| 6 | Type of operation | CO | "Status" = [Client  and operation found] | "Selection of one value from the list: [FUND]  [WITHDRAW] [TRANSFER] [CROSS] [PURCHASE] [CHARGEBACK] [B2B]  [B2C]  [C2B]  [C2C]  [C2G]  The list depends on the fields "Type of payer's payment facility"  and "Payment system" | [FUND] - depositing cash funds  [WITHDRAW] - withdrawal of funds  [TRANSFER] –  transfer of funds between homogeneous payment facilities  [CROSS] - funds transfer involving conversion  between different-type payment facilities [PURCHASE] -  purchase  [CHARGEBACK] -  chargeback  [B2B] – B2B - FPS operations  [B2C] – B2C - FPS operations  [C2B] – C2B - FPS operations  [C2C] – C2C - FPS operations  [C2G] – C2G -  FPS operations |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 7 | Information  about recipient's payment facility | Type of payment facility | CO | "Status" = [Client  and operation found] | Selection of one value from the list: [Cash] [Bank account] [Payment card] [Mobile telephone communications subscriber's number] [E-wallet]  The list depends  on the fields "Payment system" and "Type of  operation" | - |
| 8 | Bank account number | CO | Field "Status" = [Client and operation found] and "Type of payment facility" = [Bank account] | In accordance  with the format determined in Regulation of the Bank of Russia  No. 579-P | - |
| 9 | BIC of funds  to transfer funds | In accordance  with the format determined in Regulation of the Bank of Russia  No. 732-P | - |
| 10 | Number of payment card | CO | Field "Status" = [Client and operation found] and "Type of payment facility" = [Payment card] | In accordance with the format ISO/IEC 7812 | - |
| 11 | Mobile telephone communications subscriber's number | CO | Field "Status" = [Client and operation found] and "Type of payment facility" = [Mobile telephone communications subscriber's number] | In accordance  with the international numbering system and plan | - |
| 12 | E-wallet identifier | CO | Field "Status" = [Client and operation found] and "Type of payment facility"  = [E-wallet] | In accordance with the format of e-wallets identifiers determined by electronic funds operator | - |
| 13 | INN of electronic funds operator having issued an e-wallet | In accordance with the format approved by the Federal Tax Service of Russia | - |
| 14 | Information  about funds recipient's identifiers (identifying the recipient of funds) | INN (Taxpayer Identification Number) | CO | Field "Technology of funds transfer" = [INT] | In accordance with the format of the Federal Tax Service of Russia | At least one of the fields must be filled in |
| 15 | The result of calculation of the special code of ID number | The result of calculation of hash function SHA-256 |
| 16 | The result of calculation of the special code of SNILS number | The result of calculation of hash function SHA-256 | In case of availability of |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 17 |  | Mobile telephone communications subscriber's number |  |  | In accordance  with the international numbering system and plan | Mobile telephone communications subscriber's number of the funds recipient acknowledged  under cl.  5.2.1 of the Regulation  No. 683-P |
| 18 | Information determining the funds transfer operation | Date and time of operation | CO | "Status" = [Client  and operation found] | In accordance with RFC 3339 | Moscow time [UTC +03:00] |
| 19 | Amount of operation | CO | "Status" = [Client  and operation found] | Amount net of bank fees  accurate to two  decimal places | - |
| 20 | Operation currency | CO | "Status" = [Client  and operation found] | From the All-Russian currency classifier | - |
| 21 | Amount of operation  in rubles at the internal  exchange rate | CO | Field "Operation currency" ≠ [RUB] | Amount accurate to two decimal places | - |
| 22 | Purpose of payment | N | - | Text field | - |
| 23 | BIC of funds transfer operator rendering services to the funds recipient | CO | "Status" = [Client  and operation found] | In accordance  with the format determined in Regulation of the Bank of Russia  No. 732-P | - |
| 24 | Identifier of funds transfer operator rendering services to the payer, using FMS or SWIFT | CO | Field "Technology of funds transfer" = [SPFS], [SWIFT] | In accordance with SWIFT format | SWIFT-code of the payer |
| 25 | Identifier of funds transfer operator rendering services to the funds recipient, using FMS or SWIFT | In accordance with SWIFT format | SWIFT-code of the funds recipient |
| 26 | SWIFT operation identifier (operation number) | In accordance with SWIFT format | - |
| 27 | Identifier of retail and service outlet | CO | In case of operation  to the benefit of retail and service outlet | In accordance  with the format approved in the payment  system | MerchantID |
| 28 | INN of retail and service outlet | CO | In case of operation  to the benefit of retail and service outlet,  if any | In accordance with the format approved by the Federal Tax Service of Russia | - |
| 29 | Reference number of operation (transaction) | CO | Field "Technology of funds transfer" = [CARD] | In accordance  with the format approved in the payment  system | Retrieval Reference Number (RRN) |
| 30 | Operation (Transaction) response code | [Approved] [Denied] | Response Code |
| 31 | Chargeback reason code | In accordance  with the format approved in the payment  system | Reason Code |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 32 |  | BIN of funds transfer operator - acquirer |  |  | In accordance  with the format approved in the payment  system | - |
| 33 | Code reflecting the core activity of retail and service outlet | CO | Field "Technology of funds transfer" = [CARD],  and filling-in this field in authorisation messages is provided for  by PS standards | In accordance  with the format approved in the payment system | MCC |
| 34 | Token value upon a tokenised operation | CO | Field "Technology of funds transfer" = [CARD],  and a tokenised card operation  was conducted | In accordance  with the format approved in the payment system | Token Number |
| 35 | FPS identifier of funds transfer operator rendering services to the funds recipient | CO | Field "Technology of funds transfer" = [SBP], | In accordance  with FPS Operations and Payments Clearing Center (OPCC) standards | MemberID |
| 36 | FPS operation identifier (operation number) | CO | Field "Technology of funds transfer" = [SBP],  and "Type of operation" =  [C2C], [B2C] | In accordance  with FPS Operations and Payments Clearing Center (OPCC) standards | - |
| 37 | Identifier of FPS payment reference | CO | Field "Technology of funds transfer" = [SBP],  and "Type of operation" = [B2B], [C2B], and operation  was conducted using  a payment reference | In accordance  with FPS Operations and Payments Clearing Center (OPCC) standards | QRC\_ID |
| 38 | Information used  for device identification | Operation method | CO | "Status" = [Client  and operation found] | Selection of one value from the list:  [ATM] [BRANCH] [DBO]. [MB]  [DBO]. [WEB]  [DBO]. [TC] [ECOM]  [POS]  [SST] | [ATM] – using an ATM [BRANCH] - in a credit  institution branch [DBO]. [MB] - using  mobile bank [DBO]. [WEB] -  using  client bank (thin client)  [DBO]. [TC] -  using client bank (thick client)  [ECOM] - using e-commerce facilities  [POS] - using a POS-terminal [SST] - using a self-service  terminal |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 39 |  | Device identifier | CO | Field "Operation method" = [ATM], [POS] or [SST] | Text field | Unique identifier of the device used to conduct the operation |
| 40 | Address of device or credit institution branch | CO | Field "Operation method"  = [ATM], [BRANCH],  [POS] or [SST] | Text field | Address of device or credit institution branch |
| 41 | Unique numerical identifier of device on the Internet | CO | Field "Operation method"  = [DBO]. [MB], [DBO].  [WEB], [DBO]. [TC] | In accordance  with RFC 791 or RFC 2460 format | Device IP-address |
| 42 | Network address of a computer and (or) communication device (router) | N | - | In accordance with IEEE format | Device MAC-address |
| 43 | International subscriber's identifier (individual number of subscriber - natural person) | N | - | In accordance with ITU-T E. 118 format | SIM-card number (ICCID) |
| 44 | International identifier of user equipment (terminal equipment) of subscriber - natural person | N | - | In accordance with ITU-T E. 212 format | Device IMSI |
| 45 | Device digital footprint | N | - | Device digital footprint obtained in accordance  with recommendations  of the Bank of Russia | - |
| 46 | Phishing URL | N | - | In accordance with RFC 3986 format | To be filled out in case an operation is initiated from a phishing website |
| 47 | Criteria of legitimacy of operation without consent | Criteria of legitimacy of operation without consent | CO | Field "Status" = [Client and operation found] and operation meets at least one of legitimacy criteria | From the classifier  "Criteria of operation legitimacy (signs of funds transfer without consent of the client) without consent" set forth  in [Appendix 28](#_bookmark67) | All criteria of legitimacy of operation without consent shall be chosen |

APPENDIX 7. DATA PROVISION FORM REQ\_OWC\_REVERSE - FORM OF REQUEST OF THE BANK OF RUSSIA FOR THE PURPOSES OF RECEIVING INFORMATION ABOUT PAYERS TO THE FUNDS RECIPIENT SPECIFIED IN THE BANK OF RUSSIA' REQUEST

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 1 | Type of request/response | Type of request/response | O | - | [REQ\_OWC\_Reverse] | Pre-filled field |
| 2 | Information  about funds recipient's identifiers (identifying the recipient of funds) | INN (Taxpayer Identification Number) | CO | If the payer is a legal entity, otherwise, if any | In accordance with the format of the Federal Tax Service of Russia | At least one of the fields must be filled in |
| 3 | The result of calculation of the special code of ID number | CO | If the payer is an individual | The result of calculation of hash function SHA-256 |
| 4 | The result of calculation of the special code of SNILS number | CO | If the payer is an individual, if any | The result of calculation of hash function SHA-256 | - |
| 5 | Mobile telephone communications subscriber's number | CO | If the payer is an individual, otherwise, if any | In accordance  with the international numbering system and plan | Mobile telephone communications subscriber's  number of the payer acknowledged  under cl.  5.2.1 of the Regulation  No. 683-P |
| 6 | Information  about recipient's payment facility | Type of funds recipient's payment facility | O | Field "Type of operation"  = [PURCHASE], [C2B],  [B2B] to be filled in, if any | Selection of one value from the list: [Cash] [Bank account] [Payment card] [Mobile telephone communications subscriber's number] [E-wallet] | - |
| 7 | Bank account number | CO | Field "Type of payment facility" = [Bank account] | In accordance  with the format determined in Regulation of the Bank of Russia  No. 579-P | - |
| 8 | BIC of funds  to transfer funds |  |  | In accordance  with the format determined in Regulation of the Bank of Russia  No. 732-P | - |
| 9 | Number of payment card | CO | Field "Type of payment facility" = [Payment card] | In accordance with the format ISO/IEC 7812 | - |
| 10 | Mobile telephone communications subscriber's number | CO | Field "Type of payment facility" = [Mobile telephone communications subscriber's number] | In accordance  with the international numbering system and plan | - |
| 11 | E-wallet identifier | CO | Field "Type of payment facility" = [E-wallet] | In accordance with the format of e-wallets identifiers determined by electronic funds operator | - |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 12 |  | INN of electronic funds operator having issued an e-wallet |  |  | In accordance with the format approved by the Federal Tax Service of Russia | - |
| 13 | Information determining the funds transfer operation | Date and time of operation | O | - | In accordance with RFC 3339 | Moscow time [UTC +03:00] |
| 14 | Amount of operation | O | - | Amount net of bank fees  accurate to two  decimal places | - |
| 15 | Operation currency | O | - | From the All-Russian currency classifier | - |
| 16 | Identifier of funds transfer operator rendering services to the payer, using FMS or SWIFT | CO | Field "Technology of funds transfer" = [SPFS], [SWIFT] | In accordance with SWIFT format | SWIFT-code of the payer |
| 17 | Identifier of funds transfer operator rendering services to the funds recipient, using FMS or SWIFT | In accordance with SWIFT format | SWIFT-code of the funds recipient |
| 18 | SWIFT operation identifier (operation number) | In accordance with SWIFT format | - |
| 19 | Identifier of retail and service outlet | CO | In case of operation  to the benefit of retail and service outlet | In accordance  with the format approved in the payment  system | MerchantID |
| 20 | INN of retail and service outlet | CO | In case of operation  to the benefit of retail and service outlet,  if any | In accordance with the format approved by the Federal Tax Service of Russia | - |
| 21 | Reference number of operation (transaction) | CO | Field "Technology of funds transfer" = [CARD] | In accordance  with the format approved in the payment  system | Retrieval Reference Number (RRN) |
| 22 | Operation (Transaction) response code | [Approved] [Denied] | Response Code |
| 23 | Chargeback reason code | In accordance  with the format approved in the payment  system | Reason Code |
| 24 | BIN of funds transfer operator - acquirer | In accordance  with the format approved in the payment  system | - |
| 25 | Code reflecting the core activity of retail and service outlet | CO | Field "Technology of funds transfer" = [CARD],  and filling-in this field in authorisation messages is provided for  by PS standards | In accordance  with the format approved in the payment system | MCC |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 26 |  | Token value upon a tokenised operation | CO | Field "Technology of funds transfer" = [CARD],  and a tokenised card operation  was conducted | In accordance  with the format approved in the payment system | Token Number |
| 27 | FPS identifier of funds transfer operator rendering services to the funds recipient | CO | Field "Technology of funds transfer" = [SBP], | In accordance  with FPS Operations and Payments Clearing Center (OPCC) standards | MemberID |
| 28 | FPS operation identifier (operation number) | CO | Field "Technology of funds transfer" = [SBP], | In accordance  with FPS Operations and Payments Clearing Center (OPCC) standards | TR ID |
| 29 | Identifier of FPS payment reference | CO | Field "Technology of funds transfer" = [SBP]], "Type of operation' = [B2B], [C2B], [C2G], and operation  was conducted using  a payment reference | In accordance  with FPS Operations and Payments Clearing Center (OPCC) standards | QRC\_ID |
| 30 | Information about analysis of operation without consent | Number of days  before and after the specified operation, for which the funds recipient's operations are to be  operator | N | - | Integer number >0 | - |

Data provision form RESP\_OWC\_Reverse - Form of submission of response to request of the Bank of Russia for the purposes of receiving information about payers to the specified funds recipient

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 1 | Type of request/response | Type of request/response | O | - | [RESP\_OWC\_Reverse] | Pre-filled field |
| 2 | Status | Status | O | - | [Client and operation found]  [Client not found] [Operation not found]  [Additional time for consideration is  required] | - |
| 3 | Element underlying the information submitted | Element RESP\_OWC\_ Reverse underlying the information submitted | CO | "Status" = [Client  and operation found] | One or the aggregate of values specified  in the request  divided ";" | - |
| 4 | Information about payer having transferred funds to the funds recipient, depending on the method of funds transfer implementation | Type of funds recipient's payment facility | CO | "Status" = [Client  and operation found] | Selection of one value from the list: [Cash] [Bank account] [Payment card] [Mobile telephone communications subscriber's number] [E-wallet] | - |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 5 |  | Bank account number | CO | Field "Type of payment facility" = [Bank account] | In accordance  with the format determined in Regulation of the Bank of Russia  No. 579-P | - |
| 6 | BIC of funds  to transfer funds | In accordance  with the format determined in Regulation of the Bank of Russia  No. 732-P | - |
| 7 | Number of payment card | CO | Field "Type of payment facility" = [Payment card] | In accordance with the format ISO/IEC 7812 | - |
| 8 | Mobile telephone communications subscriber's number | CO | Field "Type of payment facility" = [Mobile telephone communications subscriber's number] | In accordance  with the international numbering system and plan | - |
| 9 | E-wallet identifier | CO | Field "Type of payment facility" = [E-wallet] | In accordance with the format of e-wallets identifiers determined by electronic funds operator | - |
| 10 | INN of electronic funds operator having issued an e-wallet | In accordance with the format approved by the Federal Tax Service of Russia | - |
| 11 | Criteria of legitimacy of operation without consent characterising the payer | Criteria of legitimacy of operation without consent characterising the payer | CO | Field "Status" = [Client and operation found] and payer meets at least one of legitimacy criteria | From the classifier  "Criteria of operation legitimacy (signs of funds transfer without consent of the client) without consent" set forth  in [Appendix 28](#_bookmark67) | All criteria of legitimacy of operation without consent characterising the payer shall be chosen |
| 12 | Information about operation method | Technology of funds transfer | CO | "Status" = [Client  and operation found] | Selection of one value from the list:  [INT]  [CARD] [WALLET] [PS BR]  [SPFS] [SWIFT] [SBP] [MONEY]  The list depends  on the field "Type of payer's payment facility" | [INT] – internal transfer  [CARD] - card payment systems [WALLET] - payment systems without account opening [PS\_BR] - inter-bank transfers using the Payment System of te Bank of Russia  [SPFS] - inter-bank transfers using FMS (Financial Messaging System)  [SWIFT] - inter-bank transfers using SWIFT  [SBP] - inter-bank transfers using FPS [MONEY] - faster payments  without account opening |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 13 |  | Payment system | CO | Field "Status" = [Client and operation found] and "Technology of funds transfer" = [CARD], [WALLET], [MONEY] | INN, in accordance with the format of the Federal Tax Service of Russia, or [Other] | In case of availability of INN for a payment system operator or electronic funds operator, INN is to be specified, otherwise [Other] |
| 14 | Type of operation | CO | "Status" = [Client  and operation found] | Selection of one value from the list: [FUND]  [WITHDRAW] [TRANSFER] [CROSS] [PURCHASE] [CHARGEBACK] [B2B]  [B2C]  [C2B]  [C2C]  [C2G]  The list depends on the fields "Type of payer's payment facility"  and "Payment system" | [FUND] - depositing cash funds  [WITHDRAW] - withdrawal of funds  [TRANSFER] –  transfer of funds between homogeneous payment facilities  [CROSS] - funds transfer involving conversion  between different-type payment facilities [PURCHASE] -  purchase  [CHARGEBACK] -  chargeback  [B2B] – B2B - FPS operations  [B2C] – B2C - FPS operations  [C2B] – C2B - FPS operations  [C2C] – C2C - FPS operations  [C2G] – C2G -  FPS operations |
| 15 | Information determining the funds transfer operation | Date and time of operation | O | "Status" = [Client  and operation found] | In accordance with RFC 3339 | Moscow time [UTC +03:00] |
| 16 | Amount of operation | O | "Status" = [Client  and operation found] | Amount net of bank fees  accurate to two  decimal places | - |
| 17 | Operation currency | O | "Status" = [Client  and operation found] | From the All-Russian currency classifier | - |
| 18 | Identifier of funds transfer operator rendering services to the payer, using FMS or SWIFT | CO | Field "Technology of funds transfer" = [SPFS], [SWIFT] | In accordance with SWIFT format | SWIFT-code of the payer |
| 19 | Identifier of funds transfer operator rendering services to the funds recipient, using FMS or SWIFT | In accordance with SWIFT format | SWIFT-code of the funds recipient |
| 20 | SWIFT operation identifier (operation number) | In accordance with SWIFT format | - |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 21 |  | Identifier of retail and service outlet | CO | In case of operation  to the benefit of retail and service outlet | In accordance  with the format approved in the payment  system | MerchantID |
| 22 | INN of retail and service outlet | CO | In case of operation  to the benefit of retail and service outlet,  if any | In accordance with the format approved by the Federal Tax Service of Russia | - |
| 23 | Reference number of operation (transaction) | CO | Field "Technology of funds transfer" = [CARD] | In accordance  with the format approved in the payment  system | Retrieval Reference Number (RRN) |
| 24 | Operation (Transaction) response code | [Approved] [Denied] | Response Code |
| 25 | Chargeback reason code | In accordance  with the format approved in the payment  system | Reason Code |
| 26 | BIN of funds transfer operator - acquirer | In accordance  with the format approved in the payment  system | - |
| 27 | Code reflecting the core activity of retail and service outlet | CO | Field "Technology of funds transfer" = [CARD],  and filling-in this field in authorisation messages is provided for  by PS standards | In accordance  with the format approved in the payment system | MCC |
| 28 | Token value upon a tokenised operation | CO | Field "Technology of funds transfer" = [CARD],  and a tokenised card operation  was conducted | In accordance  with the format approved in the payment system | Token Number |
| 29 | FPS identifier of funds transfer operator rendering services to the funds recipient | CO | Field "Technology of funds transfer" = [SBP], | In accordance  with FPS Operations and Payments Clearing Center (OPCC) standards | MemberID |
| 30 | FPS operation identifier (operation number) | CO | Field "Technology of funds transfer" = [SBP],  and "Type of operation" =  [C2C], [B2C] | In accordance  with FPS Operations and Payments Clearing Center (OPCC) standards | - |
| 31 | Identifier of FPS payment reference | CO | Field "Technology of funds transfer" = [SBP],  and "Type of operation" = [B2B], [C2B], and operation  was conducted using  a payment reference | In accordance  with FPS Operations and Payments Clearing Center (OPCC) standards | QRC\_ID |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 32 | Criteria of legitimacy of operation without consent | Criteria of legitimacy of operation without consent | CO | Field "Status" = [Client and operation found] and operation meets at least one of legitimacy criteria | From the classifier  "Criteria of operation legitimacy (signs of funds transfer without consent of the client) without consent" set forth  in [Appendix 28](#_bookmark67) | All criteria of legitimacy of operation without consent shall be chosen |

APPENDIX 8. DATA PROVISION FORM REQ\_OWC\_REVIEW - FORM

OF REQUEST OF AN INFORMATION EXCHANGE PARTICIPANT IN CASE OF UNREASONABLE SUBMISSION TO THE BANK OF RUSSIA OF INFORMATION ON TRANSFERS WITHOUT CONSENT

OF THE CLIENT

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 1 | Type of notification | Type of notification | O | - | [REQ\_OWC\_Review] | Pre-filled field |
| 2 | Information identifying the client included in the database about cases  and attempts of funds transfers without the client's consent | INN (Taxpayer Identification Number) | CO | If the payer is a legal entity, otherwise, if any | In accordance with the format of the Federal Tax Service of Russia | At least one of the fields must be filled in |
| 3 | The result of calculation of the special code of ID number | CO | If the payer is an individual | The result of calculation of hash function SHA-256 |
| 4 | The result of calculation of the special code of SNILS number | CO | If the payer is an individual, if any | The result of calculation of hash function SHA-256 | - |
| 5 | Mobile telephone communications subscriber's number | CO | If the payer is an individual, otherwise, if any | In accordance  with the international numbering system and plan | Mobile telephone communications subscriber's  number of the payer acknowledged  under cl.  5.2.1 of the Regulation  No. 683-P |
| 6 | Information about the client included  in the database  about cases and attempts of funds transfers without the client's consent, depending on the funds transfer method | Bank account number | CO | Field "Type of payment facility" = [Bank account] | In accordance  with the format determined in Regulation of the Bank of Russia  No. 579-P | The required data of the client are to be specified characterising the client's payment facility  depending on the funds transfer method  One of the fields must be filled in |
| 7 | BIC of funds  to transfer funds | In accordance  with the format determined in Regulation of the Bank of Russia  No. 732-P |
| 8 | Number of payment card | CO | Field "Type of payment facility" = [Payment card] | In accordance with the format ISO/IEC 7812 |
| 9 | Mobile telephone communications subscriber's number | CO | Field "Type of payment facility" = [Mobile telephone communications subscriber's number] | In accordance  with the international numbering system and plan |
| 10 | E-wallet identifier | CO | Field "Type of payment facility" = [E-wallet] | In accordance with the format of e-wallets identifiers determined by electronic funds operator |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 11 |  | INN of electronic funds operator having issued an e-wallet |  |  | In accordance with the format approved by the Federal Tax Service of Russia |  |
| 12 | Identifier of retail and service outlet | CO | In case of operation  to the benefit of retail and service outlet | In accordance  with the format approved in the payment  system |
| 13 | INN of retail and service outlet | CO | In case of operation  to the benefit of retail and service outlet,  if any | In accordance with the format approved by the Federal Tax Service of Russia |
| 14 | Reasoned substantiation | Reasoned substantiation | O | - | Text field | - |

Data provision form RESP\_OWC\_Review - Form of submission of response to request of an information exchange participant in case of unreasonable submission to the Bank of Russia of information on transfers without consent of the client

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 1 | Type of notification | Type of notification | O | - | [RESP\_OWC\_Review] | Pre-filled field |
| 2 | Status of request consideration | Status of request consideration | O | - | [Accepted] [Dismissed] | - |
| 3 | Information identifying the client excluded from the database about cases  and attempts of funds transfers without the client's consent | INN (Taxpayer Identification Number) | CO | If the payer is a legal entity, otherwise, if any | In accordance with the format of the Federal Tax Service of Russia | One of the fields must be filled in |
| 4 | The result of calculation of the special code of ID number | CO | If the payer is an individual | The result of calculation of hash function SHA-256 |
| 5 | The result of calculation of the special code of SNILS number | CO | If the payer is an individual, if any | The result of calculation of hash function SHA-256 |
| 6 | Mobile telephone communications subscriber's number | CO | If the payer is an individual, otherwise, if any | In accordance  with the international numbering system  and plan |
| 7 | Information about the client excluded from the database  about cases and attempts of funds transfers without the client's consent, depending on the funds transfer method | Bank account number | CO | Field "Type of payment facility" = [Bank account] | In accordance  with the format determined in Regulation of the Bank of Russia  No. 579-P | The required data of the client are to be specified characterising the client's payment facility  depending on the funds transfer method |
| 8 | BIC of funds  to transfer funds | In accordance  with the format determined in Regulation of the Bank of Russia  No. 732-P |
| 9 | Number of payment card | CO | Field "Type of payment facility" = [Payment card] | In accordance with the format ISO/IEC 7812 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 10 |  | Mobile telephone communications subscriber's number | CO | Field "Type of payment facility" = [Mobile telephone communications subscriber's number] | In accordance  with the international numbering system and plan |  |
| 11 | E-wallet identifier | CO | Field "Type of payment facility" = [E-wallet] | In accordance with the format of e-wallets identifiers determined by electronic funds operator |
| 12 | INN of electronic funds operator having issued an e-wallet | In accordance with the format approved by the Federal Tax Service of Russia |
| 13 | Identifier of retail and service outlet | CO | In case of operation  to the benefit of retail and service outlet | In accordance  with the format approved in the payment  system |
| 14 | INN of retail and service outlet | CO | In case of operation  to the benefit of retail and service outlet,  if any | In accordance with the format approved by the Federal Tax Service of Russia |
| 15 | Substantiation | Substantiation | CO | "Status of request consideration" = [Dismissed] or, where necessary | Text field | - |

APPENDIX 9. DATA PROVISION FORM REQ\_OWC\_CORRECTION -

FORM OF REQUEST OF THE BANK OF RUSSIA ON REPEATED PROVISION OF INFORMATION ABOUT TRANSFERS WITHOUT CONSENT OF THE CLIENT

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 1 | Type of request/response | Type of request/response | O | - | [REQ\_OWC\_Correction] | Pre-filled field |
| 2 | Identifier of notification or response | Identifier of notification or response of an information exchange participant | O | - | In accordance  with AIPS FinTsERT format | Identifier of notification or response to the request previously sent to FinTsERT by an information exchange participant and containing information requiring specification or correction |
| 3 | Status | Status | O | - | [Client not found] [Operation not found] | - |
| 4 | Information requiring specification | INN (Taxpayer Identification Number) | CO | Fields from notification or response of an information exchange participant requiring specification are to be filled in.  At least one of the fields is to be filled in | In accordance with the format of the Federal Tax Service of Russia | At least one of the fields must be filled in |
| 5 | The result of calculation of the special code of ID number | The result of calculation of hash function SHA-256 |
| 6 | The result of calculation of the special code of SNILS number | The result of calculation of hash function SHA-256 | - |
| 7 | Mobile telephone communications subscriber's number | In accordance  with the international numbering system and plan | Mobile telephone communications subscriber's number of the payer acknowledged under cl. 5.2.1 of Regulation No. 683-P |
| 8 | Bank account number | In accordance  with the format determined in Regulation of the Bank of Russia  No. 579-P | - |
| 9 | BIC of funds  to transfer funds | In accordance  with the format determined in Regulation of the Bank of Russia  No. 732-P | - |
| 10 | Number of payment card | In accordance with the format ISO/IEC 7812 | - |
| 11 | Mobile telephone communications subscriber's number | In accordance  with the international numbering system  and plan | - |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 12 |  | E-wallet identifier |  |  | In accordance with the format of e-wallets identifiers determined by electronic funds operator | - |
| 13 | INN of electronic funds operator having issued an e-wallet | In accordance with the format approved by the Federal Tax Service of Russia | - |
| 14 | Date and time of operation | In accordance with RFC 3339 | Moscow time [UTC +03:00] |
| 15 | Amount of operation | Amount net of bank fees  accurate to two  decimal places | - |
| 16 | Operation currency | From the All-Russian currency classifier | - |
| 17 | Amount of operation  in rubles at the internal  exchange rate | Amount accurate to two decimal places | - |
| 18 | Purpose of payment | Text field | - |
| 19 | BIC of funds transfer operator rendering services to the funds recipient | In accordance  with the format determined in Regulation of the Bank of Russia  No. 732-P | - |
| 20 | Identifier of funds transfer operator rendering services to the payer, using FMS or SWIFT | In accordance with SWIFT format | SWIFT-code of the payer |
| 21 | Identifier of funds transfer operator rendering services to the funds recipient, using FMS or SWIFT | In accordance with SWIFT format | SWIFT-code of the funds recipient |
| 22 | SWIFT operation identifier (operation number) | In accordance with SWIFT format | - |
| 23 | Identifier of retail and service outlet | In accordance  with the format approved in the payment  system | MerchantID |
| 24 | INN of retail and service outlet | In accordance with the format approved by the Federal Tax Service of Russia | - |
| 25 | Reference number of operation (transaction) | In accordance  with the format approved in the payment  system | Retrieval Reference Number (RRN) |
| 26 | Operation (Transaction) response code | [Approved] [Denied] | Response Code |
| 27 | Chargeback reason code | In accordance  with the format approved in the payment  system | Reason Code |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 28 |  | BIN of funds  transfer  operator - acquirer |  |  | In accordance  with the format approved  in the payment  system | - |
|  |  |
|  |  |
| 29 | Code reflecting the core  activity  of retail and service  outlet | In accordance  with the format approved  in the payment  system | MCC |
|  |  |
|  |  |
|  |  |
| 30 | Token value upon  a tokenised  operation | In accordance with the format approved  in the payment  system | Token Number |
|  |  |
|  |  |
| 31 | FPS identifier  of funds  transfer  operator rendering  services to the funds  recipient | In accordance  with FPS Operations and Payments Clearing Center (OPCC)  standards | MemberID |
|  |  |
|  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| 32 | Identifier  of FPS operation (number of  operation) | In accordance  with FPS Operations and Payments Clearing Center (OPCC)  standards | - |
|  |  |
|  |  |
| 33 | Identifier of FPS payment reference | In accordance  with FPS Operations and Payments Clearing Center (OPCC)  standards | QRC\_ID |

Data provision form RESP\_OWC\_Correction - Form of submission of response to the Bank of Russia's request on repeated submission of information about transfers without consent of the client

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 1 | Type of request/response | Type of request/response | O | - | [RESP\_OWC\_  Correction] | Pre-filled field |
| 2 | Specified or | INN (Taxpayer Identification Number) | CO | At least one | In accordance with the format  of the Federal Tax Service of Russia | At least one of the fields is  of the fields |
|  | corrected |  |  | is to be |
|  | information about |  |  | filled in. |
|  | operation |  |  |  |
|  |  |  | Fields part of  specification  or correction request previously sent to an information  exchange  participant which  were specified or  corrected |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| 3 |  | The result of calculation of the special  code of ID number | The result of calculation of  hash function  SHA-256 |  |
|  |  |  |  |  |
|  |  |  |  |  |
| 4 |  | The result of calculation of the special  code of SNILS number |  |  | The result of calculation of hash function  SHA-256 | - |
|  |  |  |  |
|  |  |  |  |
| 5 |  | Mobile telephone  communications  subscriber's number |  |  | In accordance  with the international  numbering system  and plan | Mobile telephone  communications  subscriber's number  of the payer acknowledged under cl. 5.2.1  of Regulation No. 683-P |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| 6 |  | Bank account number |  |  | In accordance  with the format determined in the Regulation  of the Bank of Russia  No. 579-P | - |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 7 |  | BIC of funds  to transfer funds |  |  | In accordance  with the format determined in Regulation of the Bank of Russia  No. 732-P | - |
|  |  |
|  |  |
|  |  |  |
|  |  |  |
| 8 | Number of payment card | In accordance with the format ISO/IEC 7812 | - |
| 9 | Mobile telephone | In accordance  with the international  numbering system  and plan | - |
|  | communications |  |
|  | subscriber's number |  |
| 10 | E-wallet identifier | In accordance with the format of e-wallets  identifiers determined by electronic  funds operator | - |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| 11 | INN of electronic funds  operator having issued an  e-wallet | In accordance with the format approved by the Federal Tax Service of Russia | - |
|  |  |
|  |  |
|  |  |
|  |  |
| 12 | Date and time of operation | In accordance with RFC 3339 | Moscow time [UTC +03:00] |
| 13 | Amount of operation | Amount net of bank fees  accurate to two  decimal places | - |
|  |  |  |
|  |  |  |
|  |  |  |
| 14 | Operation currency | From the All-Russian  currency  classifier | - |
|  |  |  |
|  |  |  |
| 15 | Amount of operation | Amount accurate  to two decimal  places | - |
|  | in rubles at the internal |  |
|  | exchange rate |  |
| 16 | Purpose of payment | Text field | - |
| 17 | BIC of funds transfer  operator rendering services to the recipient of  funds | In accordance with the format determined in Regulation No. 732-P of the Bank of Russia | - |
|  |  |
|  |  |
|  |  |
|  |  |
| 18 | Identifier of funds transfer  operator  rendering services to  the payer, when  using FMS  or SWIFT | In accordance with SWIFT format | SWIFT-code of the payer |
|  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| 19 | Identifier of funds transfer  operator  rendering services to  the funds recipient  when using  FMS or SWIFT | In accordance with SWIFT format | SWIFT-code of the funds recipient |
|  |
|  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| 20 | SWIFT operation identifier (operation number) | In accordance with SWIFT format | - |
| 21 | Identifier  of retail and service  outlet | In accordance  with the format approved  in the payment  system | MerchantID |
|  |  |
|  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 22 |  | INN of retail and service outlet |  |  | In accordance with the format approved by the Federal Tax Service of Russia | - |
| 23 | Reference number | In accordance  with the format approved in the payment  system | Retrieval Reference  Number (RRN) |
| of operation (transaction) |
| 24 | Operation (Transaction) response code | [Approved] [Denied] | Response Code |
| 25 | Chargeback reason code | In accordance  with the format approved in the payment  system | Reason Code |
|  |  |  |
|  |  |  |
| 26 | BIN of funds transfer  operator - acquirer | In accordance  with the format approved in the payment  system | - |
|  |  |
|  |  |
| 27 | Code reflecting  the core  activity  of retail and service  outlet | In accordance  with the format approved in the payment  system | MCC |
|  |  |
|  |  |
|  |  |
| 28 | Token value upon  a tokenised  operation | In accordance  with the format approved  in the payment  system | Token Number |
|  |  |
|  |  |
| 29 | FPS identifier  of funds  transfer  operator rendering  services to the funds  operator | In accordance  with FPS Operations and Payments Clearing Center (OPCC)  standards | MemberID |
|  |  |
|  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| 30 | Identifier of FPS operation (number of  operation) | In accordance  with FPS Operations and Payments Clearing Center (OPCC)  standards | - |
|  |  |
|  |  |
| 31 | Identifier of FPS payment reference | In accordance  with FPS Operations and Payments Clearing Center (OPCC)  standards | QRC\_ID |

APPENDIX 10. DATA PROVISION FORM NTF\_OWC\_DATAUPDATE - FORM OF PROVISION BY INFORMATION EXCHANGE PARTICIPANTS OF ANY ADDITIONAL AND (OR) MORE DETAILED DATA IN RESPECT OF ANY INFORMATION EARLIER SUBMITTED

ABOUT TRANSFERS WITHOUT CLIENT'S CONSENT (TERMINATION OF BANK ACCOUNT, PAYMENT CARD, MOBILE TELEPHONE COMMUNICATIONS

SUBSCRIPTION AGREEMENT OR ELECTRONIC PAYMENT FACILITY AS WELL AS REPLACEMENT OF IDENTITY DOCUMENT NUMBER OR

MOBILE TELEPHONE COMMUNICATIONS SUBSCRIBER'S NUMBER OF THE CLIENT INCLUDED IN THE DATABASE OF CASES AND ATTEMPTS OF FUNDS TRANSFERS WITHOUT CONSENT OF THE CLIENT)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 1 | Type of notification | Type of notification | O | - | [NTF\_OWC\_  DataUpdate] | Pre-filled field |
| 2 | Type of operation | Type of modification of client information | O | - | [EXPIRE] [BLOCK] [REPLACE] | [EXPIRE] - in case of termination of a payment card or an electronic payment facility  due to expiry of the period of validity [BLOCK] - in case of termination of a bank account, payment card, mobile telephone communications subscription agreement or electronic payment facility due to  blocking [REPLACE] - in case of replacement of identity document number or mobile telephone communications subscriber's number of the client |
| 3 | Date and time | Date and time of expiry/replacement | O | - | In accordance with RFC 3339 | Moscow time [UTC +03:00] |
| 4 | Identification data of the client | The result of calculation of the special code of ID number | CO | In case of NP (natural person) | The result of calculation of hash function SHA-256 | One of the fields must be filled in |
| 5 | INN (Taxpayer Identification Number) | If LE | In accordance with the format of the Federal Tax Service of Russia |
| 6 | Information about the client having become obsolete due to expiry or replacement | Bank account number | CO | In case of termination of a bank account | In accordance  with the format determined in Regulation of the Bank of Russia  No. 579-P | - |
| 7 | Number of payment card | CO | In case of termination of a payment card | In accordance with the format ISO/IEC 7812 | - |
| 8 | Mobile telephone communications subscriber's number | CO | In case of expiry or replacement of a mobile telephone communications subscriber's number | In accordance with the Russian numbering system  and plan | - |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 9 |  | E-wallet identifier | CO | In case of termination of  an  e-wallet | In accordance with the format of e-wallets  determined  by electronic  funds operator | - |
|  |  |
|  |  |
|  |  |
|  |  |  |
|  |  |  |  |
| 10 | Name of electronic  funds  operator  having issued the  e-wallet | CO | Field "Identifier of  e-wallet  is filled in.  At least one  of the fields is to be filled in | From the list of electronic  funds  operators  placed  on the website of the Bank  of Russia | - |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| 11 | INN of electronic  funds  operator having  issued the  e-wallet |  |  | In accordance with the format  approved  by the Federal Tax Service of Russia | - |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |  |
| 12 | Up-to-Date information | The result of calculation of the special code of ID number | CO | "Type of modification of client information"  = [REPLACE] and replacement of identity document  number | The result of calculation of hash function SHA-256 | - |
| 13 | Mobile telephone communications subscriber's number | "Type of modification of client information"  = [REPLACE], and replacement of mobile telephone communications  subscriber's number | In accordance with the Russian numbering system  and plan | - |

STO BR BFBO-1.5-2023 85

APPENDIX 11. LIST OF TYPES OF INFORMATION SECURITY INCIDENTS AGREED WITH THE FEDERAL

EXECUTIVE AUTHORITY LIABLE FOR ENSURING SECURITY AND OPERATIONAL RELIABILITY INCIDENTS BROKEN DOWN BY ACTIVITIES OF CREDIT INSTITUTIONS, NON-BANKING

FINANCIAL INSTITUTIONS AND NATIONAL PAYMENT SYSTEM SUBJECTS AND THEIR CONSTITUENT TECHNOLOGICAL PROCESSES

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of type (area) of activity of tier one financial institution** | **Name of type (area) of activity of tier one financial institution** | **Code of type (area) of activity of tier two financial institution** | **Name of type (area) of activity of tier two**  **financial institution** | **Code of technological process** | **Name of technological process** | **Code of incident type** | **Code of incident** | **Name of incident** | **Notification criterion** | **Business data of information security incident** |
| [BANK] | Activity of a credit institution and non-banking credit institution | [UNI]  [BASE]  [RNKO]  [PNKO]  [NDKO] | Credit institution with universal  license  Credit institution with basic license  Settlement non-banking credit institution  Payment non-banking credit institution  Non-banking loan and deposit institution | [accept OrWithdrawal FundsPP] | Technological process ensuring attraction of deposits of funds of natural persons | [DT\_BAC] | [DT\_BAC\_ BANK\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the credit institution (signal value) | Identifying the fact of exceedance of allowable degradation share of the technological process established by the credit institution (signal value), | - |

86

STO BR BFBO-1.5-2023

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code of type (area) of activity of tier one financial institution | Name of type (area) of activity of tier one financial institution | Code of type (area) of activity of tier two financial institution | Name of type (area) of activity of tier two  financial institution | Code of technological process | Name of technological process | Code of incident type | Code of incident | Name of incident | Notification criterion | Business data of information security incident |
|  |  |  |  |  |  |  | [DT\_BAC\_ BANK\_2] | Incident related to exceedance of allowable degradation share of the technological process established by the credit institution (signal value), as well as allowable downtime and (or) degradation time of the technological process established by the credit institution (signal value) not exceeding 2 hours for banks with the asset value in excess of 500 or more billion rubles,  4 hours for banks with universal license with the asset value less than 500 billion rubles, for the period of more than 6 hours for banks with basic license | Identifying the fact of exceedance of allowable degradation share of the technological process established by the credit institution (signal value), as well as allowable downtime and (or) degradation time of the technological process established by the credit institution (signal value) not exceeding 2 hours for banks with the asset value in excess of 500 or more billion rubles,  4 hours for banks with universal license with the asset value  less than 500 billion rubles, 6 hours for banks  with basic license | - |
| [acceptOrWithdrawalFundsLP] | Technological process ensuring attraction of deposits of funds of legal entities | [DT\_BAC] | [DT\_BAC\_ BANK\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the credit institution (signal value) | Identifying the fact of exceedance of allowable degradation share of the technological process established by the credit institution (signal value), | - |

STO BR BFBO-1.5-2023 87

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code of type (area) of activity of tier one financial institution | Name of type (area) of activity of tier one financial institution | Code of type (area) of activity of tier two financial institution | Name of type (area) of activity of tier two  financial institution | Code of technological process | Name of technological process | Code of incident type | Code of incident | Name of incident | Notification criterion | Business data of information security incident |
|  |  |  |  |  |  |  | [DT\_BAC\_ BANK\_3] | Incident related to exceedance of allowable degradation share of the technological process established by the credit institution (signal value),  as well as allowable downtime and (or) degradation time of the technological process established by the credit institution (signal value) not exceeding 2 hours for banks with the asset value in excess of 500 or more billion rubles, 4 hours for banks  with universal license with the asset value less than 500 billion rubles, 6 hours for banks  with basic license, 6 hours for non-banking credit  institutions | Identifying the fact of exceedance of allowable degradation share of the technological process established by the credit institution (signal value), as well as allowable downtime and (or) degradation time of the technological process established by the credit institution (signal value) not exceeding 2 hours for banks with the asset value in excess of 500 or more billion rubles,  4 hours for banks with universal license with the asset value  less than 500 billion rubles, 6 hours for banks  with basic license, 6 hours for non-banking credit institutions | - |
| [placementOfFunds] | Technological process ensuring placement of funds of natural persons and (or) legal entities attracted as deposits on their own behalf  and at their own expense | [BAC] | [BAC\_ BANK\_4] | Incident related to placement of funds  of natural persons and (or) legal entities attracted as deposits on their own behalf  and at their own expense as a result of unauthorised access to information infrastructure facilities of the credit institution | Identifying events related to placement of funds of natural persons and (or) legal entities attracted as deposits on their own behalf  and at their own expense as a result of unauthorised access to information infrastructure facilities of the credit institution and which are recorded by the credit institution in the database of operational risk events and losses incurred as a result of such risk materialisation, under cl. 1.2  of the Regulation 716-P | No requirement to business data  of information security incident |

88

STO BR BFBO-1.5-2023

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code of type (area) of activity of tier one financial institution | Name of type (area) of activity of tier one financial institution | Code of type (area) of activity of tier two financial institution | Name of type (area) of activity of tier two  financial institution | Code of technological process | Name of technological process | Code of incident type | Code of incident | Name of incident | Notification criterion | Business data of information security incident |
|  |  |  |  |  |  | [DT\_BAC] | [DT\_BAC\_ BANK\_1] | Incident related to exceedance of allowable degradation  share of the technological  process established by  the credit institution (signal  value) | Identifying the fact of exceedance of allowable degradation share  of the technological process  established by the credit  institution (signal  value) | - |
|  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  | [DT\_BAC\_ | Incident related to exceedance  of allowable degradation  share of the technological  process established by  the credit institution  (signal value),  as well as allowable  downtime and (or) degradation time  of the technological process  established by the credit  institution (signal  value) not exceeding  2 hours for banks with the asset  value in excess  of 500 or more billion  rubles, 4 hours for banks  with universal license  with the asset value  less than 500 billion  rubles, 6 hours for banks  with basic license, 6 hours  for non-banking credit  institutions | Identifying the fact of exceedance of  allowable degradation share  of the technological process  established by the credit  institution (signal  value), as well as allowable  downtime and (or) degradation  time of the technological  process established by the credit  institution (signal  value) not exceeding  2 hours for banks with the asset  value in excess  of 500 or more billion  rubles, 4 hours for banks  with universal license  with the asset value  less than 500 billion  rubles, 6 hours for banks  with basic license, 6 hours  for non-banking credit  institutions | - |
|  | BANK\_3] |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

STO BR BFBO-1.5-2023 89

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code of type (area) of activity of tier one financial institution | Name of type (area) of activity of tier one financial institution | Code of type (area) of activity of tier two financial institution | Name of type (area) of activity of tier two  financial institution | Code of technological process | Name of technological process | Code of incident type | Code of incident | Name of incident | Notification criterion | Business data of information security incident |
|  |  |  |  | [maintainAccountPP] | Technological process ensuring opening and management of bank accounts of natural persons | [BAC] | [BAC\_ BANK\_3] | Incident related to the change of bank account balance as a result of unauthorised access to information infrastructure of the credit institution | Identifying events related to the change of bank account balance as a result of unauthorised access to information infrastructure of the credit institution which are recorded by the credit institution in the database  of operational risk events and losses incurred as a result of such risk materialisation,  under cl. 1.2 of the Regulation  716-P | No requirement to business data  of information security incident |
| [DT\_BAC] | [DT\_BAC\_ BANK\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the credit institution (signal value) | Identifying the fact of exceedance of allowable degradation share of the technological process established by the credit institution (signal value), | - |
| [DT\_BAC\_ BANK\_4] | Incident related to exceedance of allowable degradation share of the technological process established by the credit institution (signal value), as well as allowable downtime and (or) degradation time of the technological process established by the credit institution (signal value) not exceeding 2 hours  (except for non-banking credit institutions) | Identifying the fact of exceedance of allowable degradation share of the technological process established by the credit institution (signal value), as well as allowable downtime and (or) degradation time of the technological process established by the credit institution (signal value)  not exceeding 2 hours (except for non-banking credit institutions) | - |

90

STO BR BFBO-1.5-2023

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code of type (area) of activity of tier one financial institution | Name of type (area) of activity of tier one financial institution | Code of type (area) of activity of tier two financial institution | Name of type (area) of activity of tier two  financial institution | Code of technological process | Name of technological process | Code of incident type | Code of incident | Name of incident | Notification criterion | Business data of information security incident |
|  |  |  |  | [maintainAccountLP] | Technological process ensuring opening and management of bank accounts of legal entities | [BAC] | [BAC\_ BANK\_3] | Incident related to the change of bank account balance as a result of unauthorised access to information infrastructure of the credit institution | Identifying events related to the change of bank account balance as a result of unauthorised access to information infrastructure of the credit institution which are recorded by the credit institution  in the database of operational risk events and losses incurred as a result of such risk materialisation, under cl. 1.2  of the Regulation 716-P | No requirement to business data  of information security incident |
| [DT\_BAC] | [DT\_BAC\_ BANK\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the credit institution (signal value) | Identifying the fact of exceedance of allowable degradation share of the technological process established by the credit institution (signal value), | - |
| [DT\_BAC\_ BANK\_5] | Incident related to exceedance of allowable degradation share of the technological process established by the credit institution (signal value), as well as allowable downtime  and (or) degradation time of the technological process established by the credit institution (signal value) not exceeding 2 hours | Identifying the fact of exceedance of allowable degradation share of the technological process established by the credit institution (signal value), as well as allowable downtime and (or) degradation time of the technological process established by the credit institution (signal value) not exceeding 2 hours | - |

STO BR BFBO-1.5-2023

91

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code of type (area) of activity of tier one financial institution | Name of type (area) of activity of tier one financial institution | Code of type (area) of activity of tier two financial institution | Name of type (area) of activity of tier two  financial institution | Code of technological process | Name of technological process | Code of incident type | Code of incident | Name of incident | Notification criterion | Business data of information security incident |
|  |  |  |  | [transferOfFundsByOrderPP] | Technological process ensuring funds transfers under orders of natural persons  on their bank accounts | [MTR] | [MTR\_ OPDS\_1] | Incident related to funds transfer based on an unlawfully modified order of FTO client | Identifying incidents related to funds transfers based on unlawfully modified orders of FTO client  recorded by the credit institution in the database  of operational risk events and losses incurred as a result of such risk materialisation,  under cl. 1.2 of the Regulation  716-P | No requirement to business data  of information security incident |
| [MTR\_ OPDS\_2] | Incident related to funds transfer with misrepresented details as a result of unauthorised access to information infrastructure facilities of FTO | Identifying incidents related to funds transfers with misrepresented details as a result of unauthorised access to information infrastructure facilities of FTO recorded by the credit institution in the database of operational  risk events and losses incurred as a result of such risk materialisation, under cl. 1.2 of the Regulation 716-P | No requirement to business data  of information security incident |
| [DT\_MTR] | [DT\_MTR\_ OPDS\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the credit institution (signal value) | Identifying the fact of exceedance of allowable degradation share of the technological process established by the credit institution (signal value), | - |

92

STO BR BFBO-1.5-2023

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code of type (area) of activity of tier one financial institution | Name of type (area) of activity of tier one financial institution | Code of type (area) of activity of tier two financial institution | Name of type (area) of activity of tier two  financial institution | Code of technological process | Name of technological process | Code of incident type | Code of incident | Name of incident | Notification criterion | Business data of information security incident |
|  |  |  |  |  |  |  | [DT\_MTR\_ OPDS\_2] | Incident related to exceedance of allowable degradation share of the technological process established by the credit institution (signal value),  as well as allowable downtime and (or) degradation time of the technological process established by the credit institution (signal value) not exceeding 2 hours for banks with the asset value in excess of 500 or more billion rubles or deemed significant  at the payment services market, 4 hours for banks with universal license with the asset value less than 500 billion rubles, 6 hours for banks with basic license | Identifying the fact of exceedance of allowable degradation share of the technological process established by the credit institution (signal value), as well as allowable downtime and (or) degradation time of the technological process established by the credit institution (signal value) not exceeding 2 hours for banks with the asset value in excess of 500 or more billion rubles or deemed significant  at the payment services market, 4 hours for banks with universal license with the asset value less than 500 billion rubles, 6 hours for banks with basic license | - |
| [transferOfFundsByOrderLP] | Technological process ensuring funds transfers under orders of legal entities  including correspondent banks, on their bank accounts, other than funds transfers under orders of payment system participants | [MTR] | [MTR\_ OPDS\_1] | Incident related to funds transfer based on an unlawfully modified order of FTO client | Identifying incidents related to funds transfers based on unlawfully modified orders of FTO client  recorded by the credit institution in the database  of operational risk events and losses incurred as a result of such risk materialisation,  under cl. 1.2 of the Regulation 716-P | No requirement to business data  of information security incident |

STO BR BFBO-1.5-2023 93

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code of type (area) of activity of tier one financial institution | Name of type (area) of activity of tier one financial institution | Code of type (area) of activity of tier two financial institution | Name of type (area) of activity of tier two  financial institution | Code of technological process | Name of technological process | Code of incident type | Code of incident | Name of incident | Notification criterion | Business data of information security incident |
|  |  |  |  |  |  |  | [MTR\_  OPDS\_2] | Incident related to funds  transfer  with misrepresented  details as a result of unauthorised access  to information infrastructure  facilities of FTO | Identifying incidents  related to funds  transfers  with misrepresented details  as a result of unauthorised access to information  infrastructure facilities  of FTO recorded  by the credit institution  in the database of operational  risk events and losses  incurred as a result of such risk  materialisation, under cl. 1.2  of the Regulation 716-P | No requirement  to business data  of an information security  incident |
| [DT\_MTR] | [DT\_MTR\_ OPDS\_1] | Incident related to exceedance of allowable degradation  share of the technological  process established by  the credit institution (signal  value) | Identifying the fact of exceedance of allowable degradation share  of the technological process  established by the credit  institution (signal  value) | - |

94

STO BR BFBO-1.5-2023

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code of type (area) of activity of tier one financial institution | Name of type (area) of activity of tier one financial institution | Code of type (area) of activity of tier two financial institution | Name of type (area) of activity of tier two  financial institution | Code of technological process | Name of technological process | Code of incident type | Code of incident | Name of incident | Notification criterion | Business data of information security incident |
|  |  |  |  |  |  |  | [DT\_MTR\_ OPDS\_3] | Incident related to exceedance of allowable degradation share of the technological process established by the credit institution (signal value),  as well as allowable downtime and (or) degradation time of the technological process established by the credit institution (signal value) not exceeding 2 hours for banks with the asset value in excess of 500 or more billion rubles or deemed significant  at the payment services market, 4 hours for banks with universal license with the asset value less than 500 billion rubles, 6 hours for banks with basic license and non-banking credit institutions | Identifying the fact of exceedance of allowable degradation share of the technological process established by the credit institution (signal value), as well as allowable downtime and (or) degradation time of the technological process established by the credit institution (signal value) not exceeding 2 hours for banks with the asset value in excess of 500 or more billion rubles or deemed significant  at the payment services market, 4 hours for banks with universal license with the asset value less than 500 billion rubles, 6 hours for banks with basic license and non-banking credit institutions | - |
| [transferOfFundsWithoutAccount] | Technological process ensuring funds transfers without opening bank accounts, including electronic funds transfers (other than postal transfers) | [MTR] | [MTR\_ OPDS\_3] | Incident related  to funds transfers without opening bank accounts, including electronic funds transfers (other than postal transfers), based on unlawfully modified order of FTO client | Identifying incidents related to funds transfers without opening bank accounts,  including electronic funds transfers (other than postal transfers), based on unlawfully modified order of FTO client which are recorded by the credit institution in the database  of operational risk events and losses incurred as a result of such risk materialisation,  under cl. 1.2 of the Regulation  716-P | No requirement to business data  of information security incident |

STO BR BFBO-1.5-2023 95

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code of type (area) of activity of tier one financial institution | Name of type (area) of activity of tier one financial institution | Code of type (area) of activity of tier two financial institution | Name of type (area) of activity of tier two  financial institution | Code of technological process | Name of technological process | Code of incident type | Code of incident | Name of incident | Notification criterion | Business data of information security incident |
|  |  |  |  |  |  |  | [MTR\_  OPDS\_4] | Incident related  to funds  transfers without opening  bank accounts, including  electronic funds transfers  (other than postal  transfers) with misrepresented  details as a result of unauthorised access  to information infrastructure  facilities of FTO | Identifying incidents  related to funds  transfers  without opening bank accounts,  including electronic  funds transfers (other than  postal transfers)  with misrepresented details  as a result of unauthorised access to information  infrastructure facilities  of FTO recorded  by the credit institution  in the database of operational  risk events and losses  incurred as a result of such risk  materialisation, under cl. 1.2  of the Regulation 716-P | No requirement  to business data  of an information security  incident |
| [DT\_MTR] | [DT\_MTR\_ OPDS\_1] | Incident related to exceedance of allowable degradation  share of the technological  process established by  the credit institution (signal  value) | Identifying the fact of exceedance of allowable degradation share  of the technological process  established by the credit  institution (signal  value) | - |
|  |
|  |
|  |
|  |

96

STO BR BFBO-1.5-2023

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code of type (area) of activity of tier one financial institution | Name of type (area) of activity of tier one financial institution | Code of type (area) of activity of tier two financial institution | Name of type (area) of activity of tier two  financial institution | Code of technological process | Name of technological process | Code of incident type | Code of incident | Name of incident | Notification criterion | Business data of information security incident |
|  |  |  |  |  |  |  | [DT\_MTR\_ OPDS\_3] | Incident related to exceedance of allowable degradation share of the technological process established by the credit institution (signal value),  as well as allowable downtime and (or) degradation time of the technological process established by the credit institution (signal value) not exceeding 2 hours for banks with the asset value in excess of 500 or more billion rubles or deemed significant  at the payment services market, 4 hours for banks with universal license with the asset value less than 500 billion rubles, 6 hours for banks with basic license and non-banking credit institutions | Identifying the fact of exceedance of allowable degradation share of the technological process established by the credit institution (signal value), as well as allowable downtime and (or) degradation time of the technological process established by the credit institution (signal value) not exceeding 2 hours for banks with the asset value in excess of 500 or more billion rubles or deemed significant  at the payment services market, 4 hours for banks with universal license with the asset value less than 500 billion rubles, 6 hours for banks with basic license and non-banking credit institutions | - |
| [operationInFinancialMarket] | Technological process ensuring performance of financial  market  operations | [DT\_BAC] | [DT\_BAC\_ BANK\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the credit institution (signal value) | Identifying the fact of exceedance of allowable degradation share of the technological process established by the credit institution (signal value), | - |

STO BR BFBO-1.5-2023 97

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code of type (area) of activity of tier one financial institution | Name of type (area) of activity of tier one financial institution | Code of type (area) of activity of tier two financial institution | Name of type (area) of activity of tier two  financial institution | Code of technological process | Name of technological process | Code of incident type | Code of incident | Name of incident | Notification criterion | Business data of information security incident |
|  |  |  |  |  |  |  | [DT\_BAC\_ BANK\_6] | Incident related to exceedance of allowable degradation share of the technological process established by the credit institution (signal value), as well as allowable downtime and (or) degradation time of the technological process established by the credit institution (signal value) not exceeding 24 hours (except for non-banking credit institutions) | Identifying the fact of exceedance of allowable degradation share of the technological process established by the credit institution (signal value), as well as allowable downtime and (or) degradation time of the technological process established by the credit institution (signal value)  not exceeding 24 hours (except for non-banking credit institutions) | - |
| [cashOperation] | Technological process ensuring performance of cash operations | [BAC] | [BAC\_ BANK\_1] | Incident related to unauthorised cash disbursement by the credit institution | Identifying events related to unauthorised cash disbursement by the credit institution which are recorded  in the database of operational risk events and losses incurred as a result of such risk materialisation, under cl. 1.2  of the Regulation 716-P | No requirement to business data  of information security incident |
| [BAC\_ BANK\_2] | Incident related to unauthorised crediting of cash | Identifying events related to unauthorised crediting of cash by acceptance of cash by the credit institution which are recorded in the database of operational risk events and losses incurred as a result of such risk materialisation, under cl. 1.2 of the Regulation 716-P | No requirement to business data  of information security incident |

98

STO BR BFBO-1.5-2023

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code of type (area) of activity of tier one financial institution | Name of type (area) of activity of tier one financial institution | Code of type (area) of activity of tier two financial institution | Name of type (area) of activity of tier two  financial institution | Code of technological process | Name of technological process | Code of incident type | Code of incident | Name of incident | Notification criterion | Business data of information security incident |
|  |  |  |  |  |  | [DT\_BAC] | [DT\_BAC\_ BANK\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the credit institution (signal value) | Identifying the fact of exceedance of allowable degradation share of the technological process established by the credit institution (signal value), | - |
| [DT\_BAC\_ BANK\_4] | Incident related to exceedance of allowable degradation share of the technological process established by the credit institution (signal value), as well as allowable downtime and (or) degradation time of the technological process established by the credit institution (signal value) not exceeding 2 hours  (except for non-banking credit institutions) | Identifying the fact of exceedance of allowable degradation share of the technological process established by the credit institution (signal value), as well as allowable downtime and (or) degradation time of the technological process established by the credit institution (signal value)  not exceeding 2 hours (except for non-banking credit institutions) | - |
| [onlineServices] | Technological process ensuring operation of online remote services and access to performance of operations | [DT\_BAC] | [DT\_BAC\_ BANK\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the credit institution (signal value) | Identifying the fact of exceedance of allowable degradation share of the technological process established by the credit institution (signal value), | - |

STO BR BFBO-1.5-2023 99

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code of type (area) of activity of tier one financial institution | Name of type (area) of activity of tier one financial institution | Code of type (area) of activity of tier two financial institution | Name of type (area) of activity of tier two  financial institution | Code of technological process | Name of technological process | Code of incident type | Code of incident | Name of incident | Notification criterion | Business data of information security incident |
|  |  |  |  |  |  |  | [DT\_BAC\_ BANK\_4] | Incident related to exceedance of allowable degradation share of the technological process established by the credit institution (signal value), as well as allowable downtime and (or) degradation time of the technological process established by the credit institution (signal value) not exceeding 2 hours  (except for non-banking credit institutions) | Identifying the fact of exceedance of allowable degradation share of the technological process established by the credit institution (signal value), as well as allowable downtime and (or) degradation time of the technological process established by the credit institution (signal value)  not exceeding 2 hours (except for non-banking credit institutions) | - |
| [placementBPD] | Technological process ensuring placement and updating biometric personal data in the unified biometric system | [BAC] | [BAC\_ BANK\_5] | Incident related to violation of integrity (substitution, deletion) or reliability (entering fictitious biometric personal data) of biometric personal data | Identification by the credit institution of the fact of violation of integrity (substitution, deletion)  or reliability (entering fictitious biometric personal data) of biometric personal data | No requirement to business data  of information security incident |
| [DT\_BAC] | [DT\_BAC\_ BANK\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the credit institution (signal value) | Identifying the fact of exceedance of allowable degradation share of the technological process established by the credit institution (signal value), | - |

100

STO BR BFBO-1.5-2023

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code of type (area) of activity of tier one financial institution | Name of type (area) of activity of tier one financial institution | Code of type (area) of activity of tier two financial institution | Name of type (area) of activity of tier two  financial institution | Code of technological process | Name of technological process | Code of incident type | Code of incident | Name of incident | Notification criterion | Business data of information security incident |
|  |  |  |  |  |  |  | [DT\_BAC\_ BANK\_4] | Incident related to exceedance of allowable degradation share of the technological process established by the credit institution (signal value), as well as allowable downtime and (or) degradation time of the technological process established by the credit institution (signal value) not exceeding 2 hours  (except for non-banking credit institutions) | Identifying the fact of exceedance of allowable degradation share of the technological process established by the credit institution (signal value), as well as allowable downtime and (or) degradation time of the technological process established by the credit institution (signal value)  not exceeding 2 hours (except for non-banking credit institutions) | - |
| [usageBPDforIA] | Technological process ensuring identification and (or) authentication  using biometric personal data of natural persons, including with the use of information technologies and without personal presence | [BAC] | [BAC\_ BANK\_6] | Incident related to false-positive identification and (or) authentication using biometric personal data of natural persons, including  with the use of information technologies without their personal presence | Identification by the credit institution of the fact of false-positive identification and (or) authentication using biometric personal data of natural persons, including with the use of information technologies without their personal presence | No requirement to business data  of information security incident |
| [BAC\_ BANK\_7] | Incident related to identification and (or) authentication using biometric personal data of natural persons,  including with the use of information technologies without their personal presence, upon substitution by the natural person of biometric personal  data | Identifying by the credit institution of the fact of identification and (or) authentication  using biometric personal data of natural persons, including  with the use of information technologies without their personal presence, upon substitution by the natural person of biometric  personal data | No requirement to business data  of information security incident |

STO BR BFBO-1.5-2023 101

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code of type (area) of activity of tier one financial institution | Name of type (area) of activity of tier one financial institution | Code of type (area) of activity of tier two financial institution | Name of type (area) of activity of tier two  financial institution | Code of technological process | Name of technological process | Code of incident type | Code of incident | Name of incident | Notification criterion | Business data of information security incident |
|  |  |  |  |  |  | [DT\_BAC] | [DT\_BAC\_ BANK\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the credit institution (signal value) | Identifying the fact of exceedance of allowable degradation share of the technological process established by the credit institution (signal value), | - |
| [DT\_BAC\_ BANK\_4] | Incident related to exceedance of allowable degradation share of the technological process established by the credit institution (signal value), as well as allowable downtime and (or) degradation time of the technological process established by the credit institution (signal value) not exceeding 2 hours  (except for non-banking credit institutions) | Identifying the fact of exceedance of allowable degradation share of the technological process established by the credit institution (signal value), as well as allowable downtime and (or) degradation time of the technological process established by the credit institution (signal value)  not exceeding 2 hours (except for non-banking credit institutions) | - |
| [OPDS] | Funds transfer operator | | | Technological processes of FTO are part of technological processes of credit institutions | | | | | | - |
| [OEDS] | Electronic funds operator | | | Technological processes of EFO are part of technological processes of credit institutions | | | | | | - |
| [OUPI] | Payment infrastructure services  operator | [OC] | Operations center | [providingMessaging] | Ensuring e-message exchange upon cooperation with FTO of  FTO, IESO (information exchange services operator), PISO (CC - payment clearing center, SC - settlement center) | [MTR] | [MTR\_ OC\_1] | Incident related to funds transfer with misrepresented details based on unlawfully modified e-message of FTO, FTO, PISO client upon ensuring e-message exchange | Receiving by PISO (OC - operations center) of notifications from FTO in the form prescribed in the agreement or unaided identification of the fact of funds transfer with misrepresented details based on unlawfully modified e-message of FTO, FTO, PISO client upon ensuring e-message exchange | No requirement to business data  of information security incident |

102

STO BR BFBO-1.5-2023

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code of type (area) of activity of tier one financial institution | Name of type (area) of activity of tier one financial institution | Code of type (area) of activity of tier two financial institution | Name of type (area) of activity of tier two  financial institution | Code of technological process | Name of technological process | Code of incident type | Code of incident | Name of incident | Notification criterion | Business data of information security incident |
|  |  |  |  |  |  |  | [MTR\_ OC\_2] | Incident related to funds transfer with misrepresented details as a result of unauthorised access to information infrastructure facilities of FTO (OC) upon ensuring e-message exchange | Receiving by PISO (OC) of notifications from FTO in the form prescribed in the agreement or unaided identification of the fact of funds transfer with misrepresented details as a result of unauthorised access to information infrastructure facilities of FTO (OPCC - operations payment and clearing center) upon ensuring e-message exchange | No requirement to business data  of information security incident |
| [PKC] | Payment clearing center | [acceptanceForExecution] | Performance of the procedures for accepting e-messages of FTO, PISO (OC), IESO for execution | [MTR] | [MTR\_ OPKC\_3] | Incident related to funds transfer with misrepresented details based on unlawfully modified e-message upon performance of the procedures for accepting e-messages for execution | Receiving by PISO (PCC) of notifications in the form prescribed in the agreement or unaided identification of the fact of funds transfer with misrepresented details based on unlawfully modified e-message of FTO, FTO, PISO (OC) client upon performance of the procedures for accepting e-messages for execution | No requirement to business data  of information security incident |
| [MTR\_ OPKC\_4] | Incident related to funds transfer with misrepresented details as a result of unauthorised access to information infrastructure facilities of FTO (PCC) upon performance of the procedures for accepting e-messages for execution | Receiving by PISO (PCC) of notifications in the form prescribed in the agreement or unaided identification of the fact of funds transfer with misrepresented details as a result of unauthorised access to information infrastructure facilities of FTO (PCC) upon performance of the procedures for accepting e-messages for execution | No requirement to business data  of information security incident |

STO BR BFBO-1.5-2023 103

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code of type (area) of activity of tier one financial institution | Name of type (area) of activity of tier one financial institution | Code of type (area) of activity of tier two financial institution | Name of type (area) of activity of tier two  financial institution | Code of technological process | Name of technological process | Code of incident type | Code of incident | Name of incident | Notification criterion | Business data of information security incident |
|  |  |  |  | [determinationOfPCP] | Determination of payment clearing positions for execution of accepted e-messages | [MTR] | [MTR\_ OPKC\_5] | Incident related to performance of operations on bank (correspondent) accounts of FTO with misrepresented details based on unlawfully modified e-message of FTO, PISO (OC), IESO when generating e-messages for execution by PISO (SC) | Receiving by PISO (PCC) of notifications in the form prescribed in the agreement or unaided identification of the fact of performance of operations on bank (correspondent) accounts of FTO with misrepresented details based on unlawfully modified e-message of FTO, PISO (OC), IESO when generating e-messages for execution by PISO (SC) | No requirement to business data  of information security incident |
| [MTR\_ OPKC\_6] | Incident related to performance of operations on bank (correspondent) accounts of FTO with misrepresented details as a result of unauthorised access to information infrastructure facilities of PISO (PCC) when generating e-messages for execution by PISO (SC) | Receiving by PISO (PCC) of notifications in the form prescribed in the agreement or unaided identification of the fact of performance of operations on bank (correspondent) accounts of FTO with misrepresented details as a result of unauthorised access to information infrastructure facilities of PISO (PCC) when generating e-messages for execution by PISO (SC) | No requirement to business data  of information security incident |
| [MTR\_ OPKC\_7] | Incident related to performance of operations on bank (correspondent) accounts of FTO with misrepresented details based on unlawfully modified e-message of FTO, PISO (OC), IESO when sending FTO notices | Receiving by PISO (PCC) of notifications in the form prescribed in the agreement or unaided identification of the fact of performance of operations on bank (correspondent) accounts of FTO with misrepresented details based on unlawfully modified e-message of FTO, PISO (OC), IESO when sending FTO notices | No requirement to business data  of information security incident |

104

STO BR BFBO-1.5-2023

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code of type (area) of activity of tier one financial institution | Name of type (area) of activity of tier one financial institution | Code of type (area) of activity of tier two financial institution | Name of type (area) of activity of tier two  financial institution | Code of technological process | Name of technological process | Code of incident type | Code of incident | Name of incident | Notification criterion | Business data of information security incident |
|  |  |  |  |  |  |  | [MTR\_ OPKC\_8] | Incident related to performance of operations on bank (correspondent) accounts of FTO with misrepresented details as a result of unauthorised access to information infrastructure facilities of PISO (PCC) when sending FTO notices | Receiving by PISO (PCC) of notifications in the form prescribed in the agreement or unaided identification of the fact of performance of operations on bank (correspondent) accounts of FTO  with misrepresented details  as a result of unauthorised access to information infrastructure facilities of PISO (PCC) when sending  FTO notices | No requirement to business data  of information security incident |
| [RC] | Settlement center | [executionOfOrder] | Execution of e-messages received from PISO (PCC) upon withdrawal and crediting of funds on correspondent accounts of FTO | [MTR] | [MTR\_RC\_1] | Incident related to performance of operations on bank (correspondent) accounts of FTO based on unlawfully modified e-message of PISO (PCC) | Receiving by PISO (PCC) of notifications in the form prescribed in the agreement or unaided identification of the fact of performance of operations on bank (correspondent) accounts of FTO based on unlawfully modified e-message of PISO (PCC) | No requirement to business data  of information security incident |
| [MTR\_ RC\_2] | Incident related to performance of operations on bank (correspondent) accounts of FTO with misrepresented details as a result of unauthorised access to information infrastructure facilities of PISO (SC) | Receiving by PISO (SC) of notifications in the form prescribed in the agreement or unaided identification of the fact of performance of operations on bank (correspondent) accounts of FTO with misrepresented details as a result of unauthorised access to information infrastructure facilities of PISO (SC) | No requirement to business data  of information security incident |
| [OUIO] | Information exchange services operator | | | No requirement to notify of the incidents | | | | | | |
| [OPS] | Payment system operator | | | No requirement to notify of the incidents | | | | | | |
| [BPA] | Bank payment agent | - | | No requirement to notify of the incidents | | | | | | |
| [BPS] | Bank payment subagent | No requirement to notify of the incidents | | | | | | |

STO BR BFBO-1.5-2023 105

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code of type (area) of activity of tier one financial institution | Name of type (area) of activity of tier one financial institution | Code of type (area) of activity of tier two financial institution | Name of type (area) of activity of tier two  financial institution | Code of technological process | Name of technological process | Code of incident type | Code of incident | Name of incident | Notification criterion | Business data of information security incident |
| [PA] | Payment aggregator | | | No requirement to notify of the incidents | | | | | | |
| [PCB] | Carrying out activity of professional securities market participants | [PCB\_BRO] | Carrying out brokerage activity | [refundOfFunds] | Technological process ensuring repayment of funds to clients | [FM] | [FM\_PCB\_ BRO\_1] | Incident related to repayment to clients of funds based on the client's demand generated without its consent, in particular, based on a modified client's demand | Receiving notification  from the client or unaided identification by broker of the fact of funds transfer  based on the client's demand generated without its consent, in particular, based on a modified client's demand | Hash of ID or INN of the client (the affected party) |
| Identifier of the order  to transfer funds |
| INN of the credit institution - the recipient of the order |
| No. of recipient's account in the credit institution |
| INN of recipient's credit institution |
| [FM\_PCB\_ BRO\_2] | Incident related to repayment to clients of funds as a result of unauthorised access to broker's infrastructure or infrastructure of cooperation between the broker  and the credit institution | Receiving notification  from the client or unaided identification by broker of the fact of funds transfer  as a result of unauthorised access to broker's infrastructure or infrastructure of cooperation between the broker and the credit institution | Hash of ID or INN of the client (the affected party) |
| Identifier of the order  to transfer funds |

106

STO BR BFBO-1.5-2023

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code of type (area) of activity of tier one financial institution | Name of type (area) of activity of tier one financial institution | Code of type (area) of activity of tier two financial institution | Name of type (area) of activity of tier two  financial institution | Code of technological process | Name of technological process | Code of incident type | Code of incident | Name of incident | Notification criterion | Business data of information security incident |
|  |  |  |  |  |  |  |  |  |  | INN of the credit institution - the recipient of the order |
| No. of recipient's account in the credit institution |
| INN of recipient's credit institution |
| [DT\_FS] | [DT\_FS\_ PCB\_ BRO\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - broker | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - broker, | - |
|  | [DT\_FS\_ PCB\_ BRO\_2] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - broker, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - broker not exceeding 24 hours | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - broker, as well as allowable downtime  and (or) degradation time of the technological process established by the financial institution - broker not exceeding 24 hours | - |
|  |  |  |  | [executionOfOrders] | Technological process ensuring execution of clients' orders to perform securities transactions and entry into agreements constituting derivative financial instruments | [FM] | [FM\_PCB\_ BRO\_3] | Incident related to execution of client's order to perform a transaction generated without its consent, in particular, based on a modified client's order | Receiving notification  from the client or unaided identification by the broker of the fact of execution of client's order to perform a transaction generated without its consent, in particular, based on a modified client's order | Trader's own code |

STO BR BFBO-1.5-2023 107

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code of type (area) of activity of tier one financial institution | Name of type (area) of activity of tier one financial institution | Code of type (area) of activity of tier two financial institution | Name of type (area) of activity of tier two  financial institution | Code of technological process | Name of technological process | Code of incident type | Code of incident | Name of incident | Notification criterion | Business data of information security incident |
|  |  |  |  |  |  |  |  |  |  | Code of trader's client (the affected party) |
| Hash of ID or INN of the client (the affected party) |
| Identifier of application sent to trade organiser |
| INN of trade organiser |
| Hash of ID or INN of the client (counterparty under over-the-counter transaction) |
| Identifier of over-the-counter agreement |
| [FM\_PCB\_ BRO\_3] | Incident related to execution of client's order to perform a transaction as a result of unauthorised access to broker's infrastructure or infrastructure of cooperation between the broker and trade organiser | Receiving notification  from the client or unaided identification by the broker of the fact of execution of client's order to perform a transaction as a result of unauthorised access to broker's infrastructure or infrastructure of cooperation between the broker and trade organiser | Trader's own code |
| Code of trader's client (the affected party) |
| Hash of ID or INN of the client (the affected party) |

108

STO BR BFBO-1.5-2023

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code of type (area) of activity of tier one financial institution | Name of type (area) of activity of tier one financial institution | Code of type (area) of activity of tier two financial institution | Name of type (area) of activity of tier two  financial institution | Code of technological process | Name of technological process | Code of incident type | Code of incident | Name of incident | Notification criterion | Business data of information security incident |
|  |  |  |  |  |  |  |  |  |  | Identifier of application sent to trade organiser |
| INN of trade organiser |
| Hash of ID or INN of the client (counterparty under over-the-counter transaction) |
| Identifier of over-the-counter agreement |
| [DT\_FS] | [DT\_FS\_ PCB\_ BRO\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - broker | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - broker, | - |
| [DT\_FS\_ PCB\_ BRO\_3] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - broker, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - broker  not exceeding 2 hours for institutions liable to use an enhanced or standard information security level, 4 hours for other institutions | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - broker, as well as allowable downtime  and (or) degradation time of the technological process established by the financial institution - broker not exceeding  2 hours for institutions liable to use an enhanced or standard information security level, 4 hours for other institutions | - |

STO BR BFBO-1.5-2023 109

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code of type (area) of activity of tier one financial institution | Name of type (area) of activity of tier one financial institution | Code of type (area) of activity of tier two financial institution | Name of type (area) of activity of tier two  financial institution | Code of technological process | Name of technological process | Code of incident type | Code of incident | Name of incident | Notification criterion | Business data of information security incident |
|  |  |  |  | [accountingOfOperation] | Technological process ensuring the making of internal accounting entries | [FM] | [FM\_PCB\_ BRO\_5] | Incident related to making internal accounting entries as a result of unauthorised access to broker's infrastructure | Identification by the broker of the fact of making internal accounting entries as a result of unauthorised access  to broker's infrastructure | No requirement to business data  of information security incident |
| [DT\_FS] | [DT\_FS\_ PCB\_ BRO\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - broker | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - broker, | - |
| [DT\_FS\_ PCB\_ BRO\_4] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - broker, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - broker not exceeding 12 hours | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - broker, as well as allowable downtime  and (or) degradation time of the technological process established by the financial institution - broker not exceeding 12 hours | - |

STO BR BFBO-1.5-2023

110

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code of type (area) of activity of tier one financial institution | Name of type (area) of activity of tier one financial institution | Code of type (area) of activity of tier two financial institution | Name of type (area) of activity of tier two  financial institution | Code of technological process | Name of technological process | Code of incident type | Code of incident | Name of incident | Notification criterion | Business data of information security incident |
|  |  | [PCB\_DIL] | Carrying out dealer activity | [performanceOfDeals] | Technological process ensuring performance of securities purchase and sale transactions on its own behalf and at its own expense through public announcement of purchase and (or) selling prices of certain securities  with an obligation to purchase and (or) to sell such securities at prices declared by the person carrying out the specified activity | [FM] | [FM\_PCB\_ DIL\_1] | Incident related to performance of securities purchase and sale transactions as a result of unauthorised access to dealer's infrastructure | Identification by dealer of the fact of performance of securities purchase and sale transactions as a result of unauthorised access to dealer's infrastructure | No requirement to business data  of information security incident |
| [DT\_FS] | [DT\_FS\_ PCB\_ BRO\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - dealer | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - dealer, | - |
| [DT\_FS\_ PCB\_DIL\_2] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - dealer, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - dealer not exceeding 24 hours | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - dealer, as well as allowable downtime  and (or) degradation time of the technological process established by the financial institution - dealer not exceeding  24 hours | - |

STO BR BFBO-1.5-2023 111

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code of type (area) of activity of tier one financial institution | Name of type (area) of activity of tier one financial institution | Code of type (area) of activity of tier two financial institution | Name of type (area) of activity of tier two  financial institution | Code of technological process | Name of technological process | Code of incident type | Code of incident | Name of incident | Notification criterion | Business data of information security incident |
|  |  |  |  | [accountingOfOperation] | Technological process ensuring the making of internal accounting entries | [FM] | [FM\_PCB\_ DIL\_2] | Incident related to making internal accounting entries as a result of unauthorised access to dealer's infrastructure | Identification by the dealer of the fact of making internal accounting entries as a result of unauthorised access  to dealer's infrastructure | No requirement to business data  of information security incident |
| [DT\_FS] | [DT\_FS\_ PCB\_ BRO\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - dealer | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - dealer, | - |
| [DT\_FS\_ PCB\_DIL\_3] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - dealer, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - dealer not exceeding 12 hours | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - dealer, as well as allowable downtime  and (or) degradation time of the technological process established by the financial institution - dealer not exceeding  12 hours | - |

STO BR BFBO-1.5-2023

112

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code of type (area) of activity of tier one financial institution | Name of type (area) of activity of tier one financial institution | Code of type (area) of activity of tier two financial institution | Name of type (area) of activity of tier two  financial institution | Code of technological process | Name of technological process | Code of incident type | Code of incident | Name of incident | Notification criterion | Business data of information security incident |
|  |  | [PCB\_FDIL] | Carrying out activity of forex dealer | [performanceOfDeals] | Technological process ensuring conclusion on its own behalf and at its own expense with natural persons not being individual entrepreneurs, other than through on-exchange trading of agreements set forth in clause 1 of Article  41 of Federal Law No. 39-FZ dated April 22, 1996  "On Securities Market" | [FM] | [FM\_PCB\_ FDIL\_1] | Incident related to performance on its own behalf and at its own expense of a transaction as a result of unauthorised access  to forex dealer's infrastructure | Identification by dealer of the fact of performance on its own behalf  and at its own expense of a transaction as a result of unauthorised access to forex dealer's infrastructure | No requirement to business data  of information security incident |
| [DT\_FS] | [DT\_FS\_ PCB\_ FDIL\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - forex dealer | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - forex dealer, | - |
| [DT\_FS\_ PCB\_ FDIL\_2] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - forex dealer, as well as allowable downtime  and (or) degradation time of the technological process established by the financial institution - forex dealer not exceeding 2 hours | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - forex dealer, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - forex dealer not exceeding 2 hours | - |

STO BR BFBO-1.5-2023 113

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code of type (area) of activity of tier one financial institution | Name of type (area) of activity of tier one financial institution | Code of type (area) of activity of tier two financial institution | Name of type (area) of activity of tier two  financial institution | Code of technological process | Name of technological process | Code of incident type | Code of incident | Name of incident | Notification criterion | Business data of information security incident |
|  |  |  |  | [refundOfFunds] | Technological process ensuring repayment of funds to clients | [FM] | [FM\_PCB\_ FDIL\_2] | Incident related to repayment to clients of funds based on the client's demand generated without its consent, in particular, based on a modified client's demand | Receiving notification  from the client or unaided identification by forex dealer of the fact of funds transfer based on the client's demand generated without its consent, in particular, based on a modified client's demand | Hash of ID or INN of the client (the affected party) |
| Identifier of the order  to transfer funds |
| INN of the credit institution - the recipient of the order |
| No. of recipient's account in the credit institution |
| INN of recipient's credit institution |
| [FM\_PCB\_ FDIL\_3] | Incident related to repayment to clients of funds as a result of unauthorised access to forex dealer's infrastructure or infrastructure of cooperation between the forex dealer and the credit institution | Receiving notification  from the client or unaided identification by forex dealer of the fact of funds transfer as a result of unauthorised access  to forex dealer's infrastructure or infrastructure of cooperation between the forex dealer and the credit institution | Hash of ID or INN of the client (the affected party) |
| Identifier of the order  to transfer funds |

STO BR BFBO-1.5-2023

114

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code of type (area) of activity of tier one financial institution | Name of type (area) of activity of tier one financial institution | Code of type (area) of activity of tier two financial institution | Name of type (area) of activity of tier two  financial institution | Code of technological process | Name of technological process | Code of incident type | Code of incident | Name of incident | Notification criterion | Business data of information security incident |
|  |  |  |  |  |  |  |  |  |  | INN of the credit institution - the recipient of the order |
| No. of recipient's account in the credit institution |
| INN of recipient's credit institution |
| [DT\_FS] | [DT\_FS\_ PCB\_ FDIL\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - forex dealer | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - forex dealer, | - |
| [DT\_FS\_ PCB\_ FDIL\_3] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - forex dealer, as well as allowable downtime  and (or) degradation time of the technological process established by the financial institution - forex dealer not exceeding 24 hours | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - forex dealer, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - forex dealer not exceeding 24 hours | - |
| [accountingOfOperation] | Technological process ensuring the making of internal accounting entries | [FM] | [FM\_PCB\_ FDIL\_4] | Incident related to making internal accounting entries as a result of unauthorised access to forex dealer's infrastructure | Identification by the forex dealer of the fact of making internal  accounting entries as a result of unauthorised access to forex dealer's  infrastructure | No requirement to business data  of information security incident |
| [DT\_FS] | [DT\_FS\_ PCB\_ FDIL\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - forex dealer | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - forex dealer, | - |

STO BR BFBO-1.5-2023 115

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code of type (area) of activity of tier one financial institution | Name of type (area) of activity of tier one financial institution | Code of type (area) of activity of tier two financial institution | Name of type (area) of activity of tier two  financial institution | Code of technological process | Name of technological process | Code of incident type | Code of incident | Name of incident | Notification criterion | Business data of information security incident |
|  |  |  |  |  |  |  | [DT\_FS\_ PCB\_ FDIL\_4] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - forex dealer, as well as allowable downtime  and (or) degradation time of the technological process established by the financial institution - forex dealer not exceeding 12 hours | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - forex dealer, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - forex dealer not exceeding 12 hours | - |
| [PCB\_UCB] | Carrying out securities management activity | [performanceOfDeals] | Technological process ensuring performance of securities transactions and (or) entry into agreements constituting derivative financial instruments  to the benefit of settlor | [FM] | [FM\_PCB\_ UCB\_1] | Incident related to performance of securities transactions and (or) entry into agreements constituting derivative financial instruments as a result of unauthorised access to dealer's infrastructure | Identification by dealer of the fact of performance of securities transactions and (or) entry  into agreements constituting derivative financial instruments as a result of unauthorised access to dealer's infrastructure | Trader's own code |
| Identifier of application sent to trade organiser |
| INN of trade organiser |
| Hash of ID or INN of the client (counterparty under over-the-counter transaction) |
| Identifier of over-the-counter agreement |

STO BR BFBO-1.5-2023

116

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code of type (area) of activity of tier one financial institution | Name of type (area) of activity of tier one financial institution | Code of type (area) of activity of tier two financial institution | Name of type (area) of activity of tier two  financial institution | Code of technological process | Name of technological process | Code of incident type | Code of incident | Name of incident | Notification criterion | Business data of information security incident |
|  |  |  |  |  |  | [DT\_FS] | [DT\_FS\_ PCB\_ UCB\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - manager | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - manager, | - |
| [DT\_FS\_ PCB\_ UCB\_2] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - manager, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - manager not exceeding 4 hours | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - manager, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - manager not exceeding 4 hours | - |
| [refundOfFunds] | Technological process ensuring repayment of funds to clients | [FM] | [FM\_PCB\_ UCB\_2] | Incident related to repayment to clients of funds based on the client's demand generated without its consent, in particular, based on a modified client's demand | Receiving notification  from the client or unaided identification by manager of the fact of funds transfer  based on the client's demand generated without its consent, in particular, based on a modified client's demand | Hash of ID or INN of the client (the affected party) |
| Identifier of the order  to transfer funds |
| INN of the credit institution - the recipient of the order |
| No. of recipient's account in the credit institution |

STO BR BFBO-1.5-2023 117

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code of type (area) of activity of tier one financial institution | Name of type (area) of activity of tier one financial institution | Code of type (area) of activity of tier two financial institution | Name of type (area) of activity of tier two  financial institution | Code of technological process | Name of technological process | Code of incident type | Code of incident | Name of incident | Notification criterion | Business data of information security incident |
|  |  |  |  |  |  |  |  |  |  | INN of recipient's credit institution |
| [FM\_PCB\_ UCB\_3] | Incident related to repayment to clients of funds as a result of unauthorised access to manager's infrastructure or infrastructure of cooperation between the manager and the credit institution | Receiving notification  from the client or unaided identification by manager of the fact of funds transfer  as a result of unauthorised access to manager's infrastructure or infrastructure of cooperation between the manager and the credit institution | Hash of ID or INN of the client (the affected party) |
| Identifier of the order  to transfer funds |
| INN of the credit institution - the recipient of the order |
| No. of recipient's account in the credit institution |
| INN of recipient's credit institution |
| [DT\_FS] | [DT\_FS\_ PCB\_ UCB\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - manager | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - manager, | - |

STO BR BFBO-1.5-2023

118

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code of type (area) of activity of tier one financial institution | Name of type (area) of activity of tier one financial institution | Code of type (area) of activity of tier two financial institution | Name of type (area) of activity of tier two  financial institution | Code of technological process | Name of technological process | Code of incident type | Code of incident | Name of incident | Notification criterion | Business data of information security incident |
|  |  |  |  |  |  |  | [DT\_FS\_ PCB\_ UCB\_3] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - manager, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - manager not exceeding 24 hours | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - manager, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - manager not exceeding 24 hours | - |
| [accountingOfOperation] | Technological process ensuring the making of internal accounting entries | [FM] | [FM\_PCB\_ UCB\_4] | Incident related to making internal accounting entries as a result of unauthorised access to manager's infrastructure | Identification by the manager of the fact of making internal accounting entries as a result of unauthorised access to manager's infrastructure | No requirement to business data  of information security incident |
| [DT\_FS] | [DT\_FS\_ PCB\_ UCB\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - manager | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - manager, | - |
| [DT\_FS\_ PCB\_ UCB\_4] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - manager, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - manager not exceeding 12 hours | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - manager, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - manager not exceeding 12 hours | - |
| [PCB\_RVC] | Carrying out activity of registrar | [accountingOfOperation] | Technological process ensuring the making of accounting entries  in the register of securities  holders | [FM] | [FM\_PCB\_ RVC\_1] | Incident related to making accounting entries in the register of securities holders as a result of unauthorised access to registrar's infrastructure | Identification by the registrar of the fact of making accounting entries  in the register of securities holders as a result of unauthorised access to registrar's infrastructure | No requirement to business data  of information security incident |

STO BR BFBO-1.5-2023 119

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code of type (area) of activity of tier one financial institution | Name of type (area) of activity of tier one financial institution | Code of type (area) of activity of tier two financial institution | Name of type (area) of activity of tier two  financial institution | Code of technological process | Name of technological process | Code of incident type | Code of incident | Name of incident | Notification criterion | Business data of information security incident |
|  |  |  |  |  |  | [DT\_FS] | [DT\_FS\_ PCB\_ RVC\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - registrar | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - registrar, | - |
| [DT\_FS\_ PCB\_ RVC\_2] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - registrar, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - registrar not exceeding 24 hours | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - registrar, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - registrar not exceeding 24 hours | - |
| [checkOfRights] | Technological process ensuring reconciliation by the registrar of securities rights accounted for by the registrar  with the central depository on the nominal holder's account of the central depository | [DT\_FS] | [DT\_FS\_ PCB\_ RVC\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - registrar | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - registrar, | - |

120

STO BR BFBO-1.5-2023

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code of type (area) of activity of tier one financial institution | Name of type (area) of activity of tier one financial institution | Code of type (area) of activity of tier two financial institution | Name of type (area) of activity of tier two  financial institution | Code of technological process | Name of technological process | Code of incident type | Code of incident | Name of incident | Notification criterion | Business data of information security incident |
|  |  |  |  |  |  |  | [DT\_FS\_ PCB\_ RVC\_3] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - registrar, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - registrar not exceeding 4 hours | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - registrar, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - registrar not exceeding 4 hours | - |
| [PCB\_DEP] | Depositary activity including activity of the central depository | [accountingOfOperation] | Technological process ensuring the making of accounting entries  in accounting records | [FM] | [FM\_PCB\_ DEP\_1] | Incident related to making accounting entries in accounting records as a result of unauthorised access  to registrar's infrastructure | Identification by the depository of the fact of making accounting entries  in accounting records as a result of unauthorised access to registrar's infrastructure | No requirement to business data  of information security incident |
| [DT\_FS] | [DT\_FS\_ PCB\_ DEP\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - depository | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - depository, | - |
| [DT\_FS\_ PCB\_ DEP\_2] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - depository, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - depository not exceeding 24 hours | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - depository, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - depository not exceeding 24 hours | - |

STO BR BFBO-1.5-2023 121

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code of type (area) of activity of tier one financial institution | Name of type (area) of activity of tier one financial institution | Code of type (area) of activity of tier two financial institution | Name of type (area) of activity of tier two  financial institution | Code of technological process | Name of technological process | Code of incident type | Code of incident | Name of incident | Notification criterion | Business data of information security incident |
|  |  |  |  | [settlementOfDeals] | Technological process ensuring settlements by settlement center as a result of transactions performed  through on-exchange trading | [FM] | [FM\_PCB\_ DEP\_2] | Incident related to settlements being the result of transactions performed  through on-exchange trading,  based on a modified securities flow order sent by the clearing organisation | Receiving a notification from the clearing organisation or unaided identification by the settlement depository of the fact of settlements as a result of transactions performed through on-exchange trading,  based on a modified securities flow order sent by the clearing organisation | Identifier of securities flow order sent  to the depository upon completion of settlements  and containing modified information about the transaction |
| INN of the depository/specialised depository - the recipient of the order |
| Hash of ID or INN of the client (the recipient) |
| No. of recipient's securities account |
| INN of the depository/specialised depository of the recipient |
| [FM\_PCB\_ DEP\_3] | Incident related to settlements being the result of transactions performed  through on-exchange trading,  as a result of unauthorised access to settlement depository's infrastructure | Identification by settlement depository of the fact of settlements being the result of transactions performed through on-exchange trading, as a result of unauthorised access of settlement depository's infrastructure | Identifier of securities flow order sent  to the depository upon completion of settlements  and containing modified information  about the transaction |
| INN of the depository/specialised depository - the recipient of the order |

STO BR BFBO-1.5-2023

122

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code of type (area) of activity of tier one financial institution | Name of type (area) of activity of tier one financial institution | Code of type (area) of activity of tier two financial institution | Name of type (area) of activity of tier two  financial institution | Code of technological process | Name of technological process | Code of incident type | Code of incident | Name of incident | Notification criterion | Business data of information security incident |
|  |  |  |  |  |  |  |  |  |  | Hash of ID or INN of the client (the recipient) |
| No. of recipient's securities account |
| INN of the depository/specialised depository of the recipient |
| [DT\_FS] | [DT\_FS\_ PCB\_ DEP\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - depository | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - depository, | - |
| [DT\_FS\_ PCB\_ DEP\_3] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - depository, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - depository not exceeding 2 hours | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - depository, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - depository not exceeding 2 hours | - |
| [paymentOfDividends] | Technological process ensuring payment to the depositor of monetary income on securities, the rights whereto are accounted for by the depository, and other monetary payments due to the holders of the said securities | [FM] | [FM\_PCB\_ DEP\_4] | Incident related to payment to the depositor of monetary income as a result of unauthorised access to depository's infrastructure or infrastructure of cooperation between the depository and the credit institution | Receiving a notification from the depositor or unaided identification by the depository of the fact of payment to the depositor of monetary  income as a result of unauthorised access to depository's infrastructure or infrastructure of cooperation between the depository  and the credit institution | Hash of ID or INN of the client (the affected party) |

STO BR BFBO-1.5-2023 123

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code of type (area) of activity of tier one financial institution | Name of type (area) of activity of tier one financial institution | Code of type (area) of activity of tier two financial institution | Name of type (area) of activity of tier two  financial institution | Code of technological process | Name of technological process | Code of incident type | Code of incident | Name of incident | Notification criterion | Business data of information security incident |
|  |  |  |  |  |  |  |  |  |  | Identifier of the order  to transfer funds |
| INN of the credit institution - the recipient of the order |
| No. of recipient's account in the credit institution |
| INN of recipient's credit institution |
| [DT\_FS] | [DT\_FS\_ PCB\_ DEP\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - depository | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - depository, | - |
| [DT\_FS\_ PCB\_ DEP\_2] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - depository, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - depository not exceeding 24 hours | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - depository, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - depository not exceeding 24 hours | - |

124

STO BR BFBO-1.5-2023

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code of type (area) of activity of tier one financial institution | Name of type (area) of activity of tier one financial institution | Code of type (area) of activity of tier two financial institution | Name of type (area) of activity of tier two  financial institution | Code of technological process | Name of technological process | Code of incident type | Code of incident | Name of incident | Notification criterion | Business data of information security incident |
|  |  |  |  | [checkOfRights] | Technological process ensuring reconciliation by the central depository of securities rights accounted for by the central depository with the registrar  on the nominal holder's account of the central depository | [DT\_FS] | [DT\_FS\_ PCB\_ DEP\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - depository | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - depository, | - |
| [DT\_FS\_ PCB\_ DEP\_4] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - central depository, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - central depository not exceeding 4 hours | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - central depository, as well as allowable downtime  and (or) degradation time of the technological process established by the financial institution - central depository  not exceeding 4 hours | - |
| [TDO] | Carrying out activity of trade organiser | | | [signDeals] | Technological process ensuring conclusion of agreement between traders | [FM] | [FM\_ TDO\_1] | Incident related to conclusion of agreement between traders based on the trader's request generated without its consent, in particular, based on a modified trader's request | Receiving notification  of a trader or a clearing organisation as well as unaided identification by trade organiser of the fact of conclusion of agreement between traders based on the trader's request generated without its consent, in particular, based on a modified trader's  request | Code of the trader (affected party) |

STO BR BFBO-1.5-2023 125

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code of type (area) of activity of tier one financial institution | Name of type (area) of activity of tier one financial institution | Code of type (area) of activity of tier two financial institution | Name of type (area) of activity of tier two  financial institution | Code of technological process | Name of technological process | Code of incident type | Code of incident | Name of incident | Notification criterion | Business data of information security incident |
|  |  | | |  |  |  |  |  |  | Hash of ID or INN of the trader (the affected party) |
| Trader's code (counterparty under the transaction) |
| Hash of ID or INN of the client (counterparty under the transaction) |
| Identifier of transaction |
| INN of the clearing organisation clearing based on trading results |
| [FM\_ TDO\_2] | Incident related to conclusion of agreement between traders or formation of agreements register  as a result of unauthorised access to trade organiser's infrastructure | Receiving notification  from a trader or a clearing organisation as well as unaided identification by trade organiser of the fact of conclusion of agreement between traders or formation of agreements register as a result of unauthorised access to trade organiser's infrastructure | Code of the trader (affected party) |
| Hash of ID or INN of the trader (the affected party) |
| Trader's code (counterparty under the transaction) |

126

STO BR BFBO-1.5-2023

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code of type (area) of activity of tier one financial institution | Name of type (area) of activity of tier one financial institution | Code of type (area) of activity of tier two financial institution | Name of type (area) of activity of tier two  financial institution | Code of technological process | Name of technological process | Code of incident type | Code of incident | Name of incident | Notification criterion | Business data of information security incident |
|  |  | | |  |  |  |  |  |  | Hash of ID or INN of the client (counterparty under the transaction) |
| Identifier of transaction |
| INN of the clearing organisation clearing based on trading results |
| [DT\_FS] | [DT\_FS\_ TDO\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - trade organiser | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - trade organiser, | - |
| [DT\_FS\_ TDO\_2] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - trade organiser, as well as allowable downtime  and (or) degradation time of the technological process established by the financial institution - trade organiser not exceeding 2 hours | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - trade organiser, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - trade organiser not exceeding  2 hours | - |

STO BR BFBO-1.5-2023 127

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code of type (area) of activity of tier one financial institution | Name of type (area) of activity of tier one financial institution | Code of type (area) of activity of tier two financial institution | Name of type (area) of activity of tier two  financial institution | Code of technological process | Name of technological process | Code of incident type | Code of incident | Name of incident | Notification criterion | Business data of information security incident |
|  |  | | | [accountingOfOperation] | Technological process ensuring the keeping of the register of traders and their clients, register of requests, register of agreements concluded through on-exchange trading, register of OTC agreements | [FM] | [FM\_ TDO\_3] | Incident related to introduction of changes to the register of traders and their clients, register of requests, register of agreements concluded through on-exchange trading, register of OTC agreements as a result of unauthorised access to trade organiser's infrastructure | Receiving notification  of a trader or a clearing organisation as well as unaided identification by trade organiser of the fact of introduction of changes to the register of traders and their clients, register of requests, register of agreements concluded through on-exchange trading, register of OTC agreements as a result of unauthorised access to trade organiser's  infrastructure | - |
| [DT\_FS] | [DT\_FS\_ TDO\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - trade organiser | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - trade organiser, | - |
| [DT\_FS\_ TDO\_2] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - trade organiser, as well as allowable downtime  and (or) degradation time of the technological process established by the financial institution - trade organiser not exceeding 2 hours | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - trade organiser, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - trade organiser not exceeding  2 hours | - |
| [disclosureOfInformation] | Technological process ensuring disclosure and provision of information by trade organiser | [DT\_FS] | [DT\_FS\_ TDO\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - trade organiser | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - trade organiser, | - |

128

STO BR BFBO-1.5-2023

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of type (area) of activity of tier one financial institution** | **Name of type (area) of activity of tier one financial institution** | **Code of type (area) of activity of tier two financial institution** | **Name of type (area) of activity of tier two**  **financial institution** | **Code of technological process** | **Name of technological process** | **Code of incident type** | **Code of incident** | **Name of incident** | **Notification criterion** | **Business data of information security incident** |
|  |  | | |  |  |  | [DT\_FS\_ TDO\_2] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - trade organiser, as well as allowable downtime  and (or) degradation time of the technological process established by the financial institution - trade organiser not exceeding 2 hours | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - trade organiser, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - trade organiser not exceeding  2 hours | - |
| [CC] | Carrying out clearing activity and activity of the central counterparty | | | [determinationOfObligations] | Technological process ensuring determination of obligations to be performed | [FM] | [FM\_CC\_1] | Incident related to determination of obligations to be performed based on a modified register of agreements sent by the trade organiser | Receiving notification from a clearing participant or  a trade organiser as well as unaided identification by the clearing organisation of the fact of determination of obligations to be performed based on a modified register of agreements sent  by the trade organiser | No requirement to business data  of information security incident |
| [FM\_CC\_2] | Incident related to determination of obligations to be performed as a result of unauthorised access to the clearing organisation's infrastructure | Receiving notification from a clearing participant or  unaided identification by the clearing organisation of the fact of determination of obligations to be performed as a result of unauthorised access to the clearing  organisation's infrastructure | No requirement to business data  of information security incident |
| [DT\_FS] | [DT\_FS\_ CC\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - clearing organisation or central counterparty | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - clearing organisation or central counterparty, | - |

STO BR BFBO-1.5-2023 129

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of type (area) of activity of tier one financial institution** | **Name of type (area) of activity of tier one financial institution** | **Code of type (area) of activity of tier two financial institution** | **Name of type (area) of activity of tier two**  **financial institution** | **Code of technological process** | **Name of technological process** | **Code of incident type** | **Code of incident** | **Name of incident** | **Notification criterion** | **Business data of information security incident** |
|  |  | | |  |  |  | [DT\_FS\_ CC\_2] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - clearing organisation or central counterparty  as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - clearing organisation or central counterparty not exceeding 2 hours | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - clearing organisation or central counterparty, as well as allowable downtime  and (or) degradation time of the technological process established by the financial institution - clearing organisation or central counterparty  not exceeding 2 hours | - |
| [executionOfObligations] | Technological process ensuring commission of acts aimed  at performance of obligations to be performed | [FM] | [FM\_CC\_3] | Incident related to commission of acts aimed at performance of obligations to be performed,  based on a modified register of agreements sent by the trade organiser | Receiving notification  from a clearing participant as well as unaided identification by the clearing organisation of the fact of commission of acts aimed at performance of obligations to be performed, based on a modified register  of agreements sent by the trade organiser | Hash of ID or INN of the client (the beneficiary) |

130

STO BR BFBO-1.5-2023

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of type (area) of activity of tier one financial institution** | **Name of type (area) of activity of tier one financial institution** | **Code of type (area) of activity of tier two financial institution** | **Name of type (area) of activity of tier two**  **financial institution** | **Code of technological process** | **Name of technological process** | **Code of incident type** | **Code of incident** | **Name of incident** | **Notification criterion** | **Business data of information security incident** |
|  |  | | |  |  |  |  |  |  | When a  funds  transfer  order is sent:  Identifier  of the funds  transfer  order  INN of the credit  institution being the recipient of the  order  No. of recipient's account with the credit  institution  INN of the credit  institution of the  recipient |
| When a  securities flow  order  is sent:  Identifier  of the securities flow  order  INN of the depository/specialised  depository being  the recipient of  the order  No. of securities account  of the recipient  INN of the depository/  specialised depository  of the recipient |

STO BR BFBO-1.5-2023 131

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of type (area) of activity of tier one financial institution** | **Name of type (area) of activity of tier one financial institution** | **Code of type (area) of activity of tier two financial institution** | **Name of type (area) of activity of tier two**  **financial institution** | **Code of technological process** | **Name of technological process** | **Code of incident type** | **Code of incident** | **Name of incident** | **Notification criterion** | **Business data of information security incident** |
|  |  | | |  |  |  | [FM\_CC\_4] | Incident related to commission  of acts aimed  at performance of obligations  to be performed,  based on the register of agreements,  as a result of unauthorised access  to the clearing organisation's  infrastructure or infrastructure  of cooperation between the clearing  organisation and settlement  organisation, settlement  depository | Receiving notification  from a clearing participant as well as  unaided identification  by the clearing organisation  of the fact of commission of acts  aimed at performance  of obligations to be  performed, as a result of unauthorised access  to the clearing organisation's  infrastructure or infrastructure  of cooperation between the clearing  organisation and settlement  organisation, settlement  depository | Hash of ID or INN  of the client  (the beneficiary) |
| When a  funds  transfer  order is sent:  Identifier  of the funds  transfer  order  INN of the credit  institution being the recipient of the  order  No. of recipient's account  with the credit  institution  INN of the credit  institution of the recipient |

STO BR BFBO-1.5-2023

132

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of type (area) of activity of tier one financial institution** | **Name of type (area) of activity of tier one financial institution** | **Code of type (area) of activity of tier two financial institution** | **Name of type (area) of activity of tier two**  **financial institution** | **Code of technological process** | **Name of technological process** | **Code of incident type** | **Code of incident** | **Name of incident** | **Notification criterion** | **Business data of information security incident** |
|  |  | | |  |  |  |  |  |  | When a  securities flow  order  is sent:  Identifier  of the securities flow  order  INN of the depository/  specialised  depository being  the recipient of  the order  No. of securities account  of the recipient  INN of the depository/  specialised depository  of the recipient |
| [DT\_FS] | [DT\_FS\_ CC\_1] | Incident related to exceedance of allowable degradation  share of the technological  process established by  the financial institution -  clearing organisation or  central counterparty | Identifying the fact of exceedance of allowable degradation share  of the technological process  established by the financial  institution - clearing  organisation or central  counterparty | - |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  | [DT\_FS\_ | Incident related to exceedance  of allowable degradation  share of the technological  process established by  the financial institution -  clearing organisation or  central counterparty,  as well as allowable  downtime and (or) degradation time  of the technological process  established by the financial  institution - clearing  organisation or central  counterparty not exceeding  2 hours | Identifying the fact of exceedance of  allowable degradation share  of the technological process  established by the financial  institution - clearing  organisation or central counterparty, as well as  allowable downtime  and (or) degradation time of the technological  process established by  the financial institution -  clearing organisation or  central counterparty,  not exceeding 2 hours | - |
|  | CC\_2] |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

STO BR BFBO-1.5-2023 133

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of type (area) of activity of tier one financial institution** | **Name of type (area) of activity of tier one financial institution** | **Code of type (area) of activity of tier two financial institution** | **Name of type (area) of activity of tier two**  **financial institution** | **Code of technological process** | **Name of technological process** | **Code of incident type** | **Code of incident** | **Name of incident** | **Notification criterion** | **Business data of information security incident** |
|  |  | | | [refundOfAssets] | Technological  process ensuring  the sending  or property  return order  constituting  a security for clearing | [FM] | [FM\_CC\_5] | Incident related to  sending a property return  order constituting  a security for clearing,  based on the order  of the clearing participant generated  without its consent, in particular,  based on a modified order | Receiving notification  from a clearing participant or  unaided identification  by the clearing organisation  of the fact of sending a property  return order constituting  a security for clearing,  based on the order  of the clearing participant generated  without its consent, in particular,  based on a modified order | Hash of ID or INN  of the client (the affected  party) |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |  | When a  funds  transfer  order is sent:  Identifier  of the funds  transfer  order  INN of the credit  institution being  the recipient of  order  No. of recipient's account with the credit  institution  INN of the credit  institution of the recipient |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

134

STO BR BFBO-1.5-2023

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of type (area) of activity of tier one financial institution** | **Name of type (area) of activity of tier one financial institution** | **Code of type (area) of activity of tier two financial institution** | **Name of type (area) of activity of tier two**  **financial institution** | **Code of technological process** | **Name of technological process** | **Code of incident type** | **Code of incident** | **Name of incident** | **Notification criterion** | **Business data of information security incident** |
|  |  | | |  |  |  |  |  |  | When a  securities flow  order  is sent:  Identifier  of the securities flow  order  INN of the depository/specialised  depository being  the recipient of  the order  No. of securities account  number  INN of the depository/  specialised depository  of the recipient |
| [FM\_CC\_6] | Incident related to  sending a property return  order constituting  a security for clearing,  as a result of unauthorised access to clearing organisation's infrastructure  or infrastructure of cooperation between the clearing organisation  and the settlement organisation,  settlement depository | Receiving notification  from a clearing participant or unaided  identification by the clearing organisation of the fact  of sending a property return  order constituting  a security for clearing,  as a result of unauthorised access to clearing organisation's infrastructure  or infrastructure of cooperation  between the clearing organisation  and the settlement organisation,  settlement depository | Hash of ID or INN  of the client (the affected party) |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

STO BR BFBO-1.5-2023 135

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of type (area) of activity of tier one financial institution** | **Name of type (area) of activity of tier one financial institution** | **Code of type (area) of activity of tier two financial institution** | **Name of type (area) of activity of tier two**  **financial institution** | **Code of technological process** | **Name of technological process** | **Code of incident type** | **Code of incident** | **Name of incident** | **Notification criterion** | **Business data of information security incident** |
|  |  | | |  |  |  |  |  |  | When a  funds  transfer  order is sent:  Identifier  of the funds  transfer  order  INN of the credit  institution being  the recipient of  funds  No. of recipient's account  with the credit  institution  INN of the credit  institution of the recipient |
| When a  securities flow  order  is sent:  Identifier  of securities  flow  order  INN of the depository/  specialised depository  depository being  the recipient of  the order  No. of securities account  number  INN of the depository/  specialised depository  of the recipient |

136

STO BR BFBO-1.5-2023

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of type (area) of activity of tier one financial institution** | **Name of type (area) of activity of tier one financial institution** | **Code of type (area) of activity of tier two financial institution** | **Name of type (area) of activity of tier two**  **financial institution** | **Code of technological process** | **Name of technological process** | **Code of incident type** | **Code of incident** | **Name of incident** | **Notification criterion** | **Business data of information security incident** |
|  |  | | |  |  | [DT\_FS] | [DT\_FS\_ CC\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - clearing organisation or central counterparty | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - clearing organisation or central counterparty, | - |
| [DT\_FS\_ CC\_2] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - clearing organisation or central counterparty  as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - clearing organisation or central counterparty not exceeding 2 hours | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - clearing organisation or central counterparty, as well as allowable downtime  and (or) degradation time of the technological process established by the financial institution - clearing organisation or central counterparty  not exceeding 2 hours | - |
| [RO] | Carrying out repository activity | - | - | [accountingOTCDeals] | Technological process ensuring accounting of repo agreements, agreements constituting derivative financial instruments,  as well as other agreements, concluded other than through on-exchange trading | [FM] | [FM\_RO\_1] | Incident related to accounting of a repo agreement, agreement constituting a derivative financial instrument, or other agreement, concluded other than through on-exchange trading, based on an electronic message of the repository's client, generated without its consent, in particular, based on a modified electronic message of the repository's client | Receiving notification  from a repository's client or unaided identification by the repository of the fact of accounting of a repo agreement, agreement constituting a derivative financial instrument, or other agreement, concluded other than through on-exchange trading, based on an electronic message of the repository's client, generated without its consent, in particular, based on a modified electronic message of the repository's client | No requirement to business data  of information security incident |

STO BR BFBO-1.5-2023 137

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of type (area) of activity of tier one financial institution** | **Name of type (area) of activity of tier one financial institution** | **Code of type (area) of activity of tier two financial institution** | **Name of type (area) of activity of tier two**  **financial institution** | **Code of technological process** | **Name of technological process** | **Code of incident type** | **Code of incident** | **Name of incident** | **Notification criterion** | **Business data of information security incident** |
|  |  |  |  |  |  |  | [FM\_RO\_2] | Incident related to accounting of repo agreements, an agreement constituting a derivative financial instrument, or other agreement, concluded other than through on-exchange trading, as a result of unauthorised access to repository's infrastructure | Receiving notification  from a repository's client or unaided identification by the repository of the fact of accounting of repo agreements, an agreement constituting a derivative financial instrument, or other agreement, concluded other than through on-exchange trading, as a result of unauthorised access to repository's  infrastructure | No requirement to business data  of information security incident |
| [DT\_FS] | [DT\_FS\_ RO\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - repository | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - repository, | - |
| [DT\_FS\_ RO\_2] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - repository, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - repository not exceeding 12 hours | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - repository, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - repository not exceeding 12 hours | - |
| [transferOfRegistry] | Technological process ensuring transfer (submission) of the register kept by the repository, to the Bank of Russia or another repository | [DT\_FS] | [DT\_FS\_ RO\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - repository | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - repository, | - |

138

STO BR BFBO-1.5-2023

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of type (area) of activity of tier one financial institution** | **Name of type (area) of activity of tier one financial institution** | **Code of type (area) of activity of tier two financial institution** | **Name of type (area) of activity of tier two**  **financial institution** | **Code of technological process** | **Name of technological process** | **Code of incident type** | **Code of incident** | **Name of incident** | **Notification criterion** | **Business data of information security incident** |
|  |  |  |  |  |  |  | [DT\_FS\_ RO\_2] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - repository, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - repository not exceeding 6 hours | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - repository, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - repository not exceeding 6 hours | - |
| [RFT] | Registrar of financial transactions | [accountingOfTransaction] | Technological process ensuring accounting by the registrar of financial transactions of information on performance of financial transactions and on operations  thereunder using a financial platform | [FM] | [FM\_RFT\_1] | Incident related to accounting of performed financial transactions and operations thereunder  using a financial platform, based on an electronic message of financial platform operator, generated without its consent or based on a modified electronic message of financial platform operator | Receiving notification of a financial platform  operator or unaided identification by the registrar of financial transactions of the fact of accounting of performed financial transaction or operation thereunder  using a financial platform, based on an electronic message of financial platform operator, generated without its consent or based on a modified electronic message of financial  platform operator | No requirement to business data  of information security incident |

STO BR BFBO-1.5-2023 139

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of type (area) of activity of tier one financial institution** | **Name of type (area) of activity of tier one financial institution** | **Code of type (area) of activity of tier two financial institution** | **Name of type (area) of activity of tier two**  **financial institution** | **Code of technological process** | **Name of technological process** | **Code of incident type** | **Code of incident** | **Name of incident** | **Notification criterion** | **Business data of information security incident** |
|  |  |  |  |  |  |  | [FM\_ RFT\_2] | Incident related to accounting of performed financial transactions and operations thereunder  using a financial platform as a result of unauthorised access  to the infrastructure of the registrar of financial transactions or infrastructure of cooperation between the financial platform operator and the registrar of financial transactions | Receiving notification of a financial platform  operator or unaided identification by the registrar of financial transactions of the fact of accounting of performed financial transaction or operation thereunder  using a financial platform as a result of unauthorised access  to the infrastructure of the registrar of financial transactions or infrastructure of cooperation between the financial platform operator and the registrar of  financial transactions | No requirement to business data  of information security incident |
| [DT\_FS] | [DT\_FS\_ RFT\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - registrar of financial transactions | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - registrar of financial transactions, | - |
| [DT\_FS\_ RFT\_2] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - registrar of financial transactions, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - registrar not exceeding 2 hours | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - registrar of financial transactions, as well as allowable downtime and (or) degradation time of the technological process established by the financial  institution - registrar not exceeding 2 hours | - |

140

STO BR BFBO-1.5-2023

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of type (area) of activity of tier one financial institution** | **Name of type (area) of activity of tier one financial institution** | **Code of type (area) of activity of tier two financial institution** | **Name of type (area) of activity of tier two**  **financial institution** | **Code of technological process** | **Name of technological process** | **Code of incident type** | **Code of incident** | **Name of incident** | **Notification criterion** | **Business data of information security incident** |
| [UCB] | Carrying out activity of management  companies of an investment  fund, unit investment fund  and non-state pension fund | | | [trustManagement] | Technological  process ensuring  trust  management  of funds' property,  in particular, the exercise  of rights  certified by  securities  constituting  the funds' property | [FM] | [FM\_  UCB\_1] | Incident related to performance  of operations with funds'  property as a result of unauthorised access  to infrastructure of the management  company | Receiving notification  from a specialised  depository or fund as well as  unaided identification  by the management company  of the fact of performance of operation  with the fund's property as a result  of unauthorised access to infrastructure  of the management company | INN of the fund  (the affected  party) |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  | When a  funds  transfer  order  is sent:  Identifier  of the funds  transfer  order  INN of the credit  institution being  the recipient of  order  No. of recipient's account  with the credit  institution  INN of the credit  institution of the  recipient |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

STO BR BFBO-1.5-2023 141

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code of type (area) of activity of tier one financial institution | Name of type (area) of activity of tier one financial institution | Code of type (area) of activity of tier two financial institution | Name of type (area) of activity of tier two  financial institution | Code of technological process | Name of technological process | Code of incident type | Code of incident | Name of incident | Notification criterion | Business data of information security incident |
|  |  | | |  |  |  |  |  |  | When a  securities flow  order  is sent:  Identifier  of securities  flow  order  INN of the depository/specialised  depository being  the recipient of  the order  No. of securities account  number  INN of the depository/  specialised depository  of the recipient |
| When a request  is sent to the broker:  Identifier  of request  INN of broker |
| [DT\_FS] | [DT\_FS\_ UCB\_1] | Incident related to exceedance of allowable degradation  share of the technological  process established by  the financial institution -  by the management company | Identifying the fact of exceedance of allowable degradation share  of the technological process  established by the financial  institution - management  company | - |
|  |

142

STO BR BFBO-1.5-2023

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of type (area) of activity of tier one financial institution** | **Name of type (area) of activity of tier one financial institution** | **Code of type (area) of activity of tier two financial institution** | **Name of type (area) of activity of tier two**  **financial institution** | **Code of technological process** | **Name of technological process** | **Code of incident type** | **Code of incident** | **Name of incident** | **Notification criterion** | **Business data of information security incident** |
|  |  | | |  |  |  | [DT\_FS\_ UCB\_2] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - management company  as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - management company not exceeding  2 hours | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - management company, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - management company  not exceeding 2 hours | - |
| [exerciseOfRights] | Technological process ensuring the exercise of rights of investment unit holders | [FM] | [FM\_ UCB\_2] | Incident related to variation of rights of investment unit holders in the register of investment unit holders as a result of unauthorised access to the management company's infrastructure | Receiving notification from a specialised  depository or fund as well as unaided identification by the management company of the fact of variation of rights of investment unit holders in the register of investment unit holders as a result of unauthorised access to the infrastructure of the management  company | - |
| [FM\_ UCB\_3] | Incident related to redemption of an investment unit based on an electronic message of the investment unit holder, generated without its consent or based on a modified electronic message  of the investment unit holder | Receiving notification from a specialised  depository or fund as well as unaided identification by the management company of the fact of redemption of an investment unit based on an electronic message of the investment unit holder, generated without its consent or based on a modified electronic message  of the investment unit holder | Identifier of the order  to transfer funds |

STO BR BFBO-1.5-2023 143

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of type (area) of activity of tier one financial institution** | **Name of type (area) of activity of tier one financial institution** | **Code of type (area) of activity of tier two financial institution** | **Name of type (area) of activity of tier two**  **financial institution** | **Code of technological process** | **Name of technological process** | **Code of incident type** | **Code of incident** | **Name of incident** | **Notification criterion** | **Business data of information security incident** |
|  |  | | |  |  |  |  |  |  | INN of the credit institution - the recipient of the order |
| No. of recipient's account in the credit institution |
| INN of recipient's credit institution |
| [FM\_ UCB\_4] | Incident related to redemption of an investment unit as a result of unauthorised access to the management company's infrastructure | Receiving notification from a specialised  depository or fund as well as unaided identification by the management company  of the fact of redemption of an investment unit as a result of unauthorised access  to the management company's infrastructure | Identifier of the order  to transfer funds |
| INN of the credit institution - the recipient of the order |
| No. of recipient's account in the credit institution |
| INN of recipient's credit institution |

144

STO BR BFBO-1.5-2023

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of type (area) of activity of tier one financial institution** | **Name of type (area) of activity of tier one financial institution** | **Code of type (area) of activity of tier two financial institution** | **Name of type (area) of activity of tier two**  **financial institution** | **Code of technological process** | **Name of technological process** | **Code of incident type** | **Code of incident** | **Name of incident** | **Notification criterion** | **Business data of information security incident** |
|  |  | | |  |  |  | [FM\_ UCB\_5] | Incident related to payment of monetary compensation upon termination of fund trust management agreement as a result of unauthorised access  to the management company's infrastructure | Receiving notification from a specialised depository or fund as well as unaided identification by the management company of the fact of payment of monetary compensation upon termination of fund trust management agreement as a result of unauthorised access to the management company's infrastructure | Identifier of the order  to transfer funds |
| INN of the credit institution - the recipient of the order |
| No. of recipient's account in the credit institution |
| INN of recipient's credit institution |
| [DT\_FS] | [DT\_FS\_ UCB\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - management company | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - management company, | - |
| [DT\_FS\_ UCB\_3] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - management company  as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - management company not exceeding  24 hours | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - management company, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - management company  not exceeding 24 hours | - |

STO BR BFBO-1.5-2023 145

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of type (area) of activity of tier one financial institution** | **Name of type (area) of activity of tier one financial institution** | **Code of type (area) of activity of tier two financial institution** | **Name of type (area) of activity of tier two**  **financial institution** | **Code of technological process** | **Name of technological process** | **Code of incident type** | **Code of incident** | **Name of incident** | **Notification criterion** | **Business data of information security incident** |
|  |  | | | [accountingOfAssets] | Technological process ensuring accounting of funds' property  and control over its disposal, in particular, the process of cooperation with the specialised depository | [DT\_FS] | [DT\_FS\_ UCB\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - management company | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - management company, | - |
| [DT\_FS\_ UCB\_3] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - management company  as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - management company not exceeding  24 hours | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - management company, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - management company  not exceeding 24 hours | - |
| [SDIF] | Carrying out activity of specialised depositories of investment fund, unit investment fund  and non-state pension fund | | | [controlOfOperation] | Technological process ensuring control by the specialised depository over funds' property disposal | [FM] | [FM\_ SDIF\_1] | Incident related to agreement of illegitimate requests sent from the compromised infrastructure of the management company and (or) funds | Receiving notification  from a management company or a fund as well as unaided identification by the specialised depository of the fact of agreement of an illegitimate request sent from the compromised infrastructure  of the management company and (or) the fund | No requirement to business data  of information security incident |

146

STO BR BFBO-1.5-2023

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of type (area) of activity of tier one financial institution** | **Name of type (area) of activity of tier one financial institution** | **Code of type (area) of activity of tier two financial institution** | **Name of type (area) of activity of tier two**  **financial institution** | **Code of technological process** | **Name of technological process** | **Code of incident type** | **Code of incident** | **Name of incident** | **Notification criterion** | **Business data of information security incident** |
|  |  | | |  |  | [DT\_FS] | [DT\_FS\_ SDIF\_1] | Incident related to exceedance of allowable degradation  share of the technological  process established by  the financial institution -  specialised  depository of investment  fund, unit investment  fund and non-state  pension fund | Identifying the fact of exceedance of allowable degradation share  of the technological process  established by the financial  institution - specialised  depository  of investment fund,  unit investment  fund and non-state  pension fund | - |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  | [DT\_FS\_ | Incident related to exceedance  of allowable degradation  share of the technological  process established by  the financial institution -  specialised  depository of investment  fund, unit investment  fund and non-state  pension fund as well as  allowable downtime  and (or) degradation time of the technological  process established  by the financial institution -  specialised  depository of investment  fund, unit investment  fund and non-state  pension fund not exceeding  24 hours | Identifying the fact of exceedance of  allowable degradation share  of the technological process  established by the financial  institution - specialised  depository  of investment fund,  unit investment  fund and non-state  pension fund as well as  allowable downtime  and (or) degradation time of the technological  process established  by the financial institution -  specialised  depository of investment  fund, unit investment  fund and non-state  pension fund not exceeding  24 hours | - |
|  | SDIF\_2] |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

STO BR BFBO-1.5-2023 147

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of type (area) of activity of tier one financial institution** | **Name of type (area) of activity of tier one financial institution** | **Code of type (area) of activity of tier two financial institution** | **Name of type (area) of activity of tier two**  **financial institution** | **Code of technological process** | **Name of technological process** | **Code of incident type** | **Code of incident** | **Name of incident** | **Notification criterion** | **Business data of information security incident** |
|  |  | | | [accountingOfHolders] | Technological process ensuring the making of accounting entries  in the register of securities holders (in case of provision of services of keeping  the register of investment unit holders of unit investment funds, mortgage participation certificates) | [FM] | [FM\_ SDIF\_2] | Incident related to making accounting entries in the register of securities holders as a result of unauthorised access to registrar's infrastructure | Identification by the specialised depository of the fact of making accounting entries in the register of securities holders as a result of unauthorised access to registrar's infrastructure | No requirement to business data  of information security incident |
| [DT\_FS] | [DT\_FS\_ SDIF\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - specialised depository of investment fund, unit investment fund and non-state pension fund | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - specialised depository of investment fund, unit investment fund and non-state pension fund, | - |

148

STO BR BFBO-1.5-2023

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of type (area) of activity of tier one financial institution** | **Name of type (area) of activity of tier one financial institution** | **Code of type (area) of activity of tier two financial institution** | **Name of type (area) of activity of tier two**  **financial institution** | **Code of technological process** | **Name of technological process** | **Code of incident type** | **Code of incident** | **Name of incident** | **Notification criterion** | **Business data of information security incident** |
|  |  | | |  |  |  | [DT\_FS\_ SDIF\_2] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - specialised depository of investment fund, unit investment fund and non-state pension fund, as well as allowable downtime  and (or) degradation time of the technological process established by the financial institution - specialised depository of investment fund, unit investment fund and non-state pension fund not exceeding 24 hours | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - specialised depository of investment fund, unit investment fund and non-state pension fund, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - specialised depository of investment  fund, unit investment fund and non-state pension fund not exceeding 24 hours | - |
| [INCIF] | Carrying out activity of joint stock investment funds | | | No requirement to notify of the incidents | | | | | | |
| [NGPF] | Carrying out activity of non-state pension funds | | | [paymentsToCustomers] | Technological process ensuring remittance of payments to depositors, participants, insured persons and their successors of a non-state pension fund in terms of statutory pension insurance and non-state pension provision | [FM] | [FM\_ NGPF\_1] | Incident related to remittance of payments in terms of statutory pension insurance and non-state pension provision  as a result of unauthorised access to NSPF's infrastructure or infrastructure of cooperation between the NSPF and the credit institution | Receiving notification from a depositor, participant, insured person, successor or credit  organisation as well as unaided identification by NSPF of the fact of remittance of payments in terms of statutory pension insurance and non-state pension provision as a result of unauthorised access to NSPF's infrastructure or infrastructure of cooperation between the NSPF and the credit institution | Hash of ID or INN of the client (the affected party) |

STO BR BFBO-1.5-2023 149

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of type (area) of activity of tier one financial institution** | **Name of type (area) of activity of tier one financial institution** | **Code of type (area) of activity of tier two financial institution** | **Name of type (area) of activity of tier two**  **financial institution** | **Code of technological process** | **Name of technological process** | **Code of incident type** | **Code of incident** | **Name of incident** | **Notification criterion** | **Business data of information security incident** |
|  |  | | |  |  |  |  |  |  | Identifier of the order  to transfer funds |
| INN of the credit institution - the recipient of the order |
| No. of recipient's account in the credit institution |
| INN of recipient's credit institution |
| [DT\_FS] | [DT\_FS\_ NGPF\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - non-state pension fund | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - non-state pension fund, | - |
| [DT\_FS\_ NGPF\_2] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - non-state pension fund, as well as allowable downtime  and (or) degradation time of the technological process established by the financial institution - non-state pension fund not exceeding 24 hours | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution -  non-state pension fund, as well as allowable downtime  and (or) degradation time of the technological process established by the financial institution - non-state pension fund not exceeding  24 hours | - |

150

STO BR BFBO-1.5-2023

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of type (area) of activity of tier one financial institution** | **Name of type (area) of activity of tier one financial institution** | **Code of type (area) of activity of tier two financial institution** | **Name of type (area) of activity of tier two**  **financial institution** | **Code of technological process** | **Name of technological process** | **Code of incident type** | **Code of incident** | **Name of incident** | **Notification criterion** | **Business data of information security incident** |
|  |  | | | [transferToUCB] | Technological process ensuring transfer of pension reserves and pension accruals of the management company | [FM] | [FM\_ NGPF\_2] | Incident related to transfer of pension reserves and pension accruals of the management company as a result of unauthorised access to NSPF's infrastructure or infrastructure of cooperation between the NSPF and the credit institution | Receiving notification  from a management company or a credit institution as well as unaided identification by the NSPF of the fact of transfer of pension reserves and pension accruals of the management company as a result of unauthorised access to NSPF's infrastructure or infrastructure of cooperation between the NSPF and the credit institution | Identifier of the order  to transfer funds |
| INN of the credit institution - the recipient of the order |
| No. of recipient's account in the credit institution |
| INN of recipient's credit institution |
| [DT\_FS] | [DT\_FS\_ NGPF\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - non-state pension fund | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - non-state pension fund, | - |

STO BR BFBO-1.5-2023 151

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of type (area) of activity of tier one financial institution** | **Name of type (area) of activity of tier one financial institution** | **Code of type (area) of activity of tier two financial institution** | **Name of type (area) of activity of tier two**  **financial institution** | **Code of technological process** | **Name of technological process** | **Code of incident type** | **Code of incident** | **Name of incident** | **Notification criterion** | **Business data of information security incident** |
|  |  | | |  |  |  | [DT\_FS\_ NGPF\_2] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution -  non-state pension fund, as well as allowable downtime  and (or) degradation time of the technological process established by the financial institution - non-state pension fund not exceeding  24 hours | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution -  non-state pension fund, as well as allowable downtime  and (or) degradation time of the technological process established by the financial institution - non-state pension fund not exceeding  24 hours | - |
| [transferToNGPF] | Technological process ensuring transfer of redemption amounts (pension accrual funds) to other non-state pension funds and the Pension  Fund of the Russian Federation | [FM] | [FM\_ NGPF\_3] | Incident related to transfer of redemption amounts as a result of unauthorised access to NSPF's infrastructure or infrastructure of cooperation between the NSPF and the credit institution | Receiving notification  from a credit institution or unaided identification by the NSPF of the fact of transfer of redemption amounts as a result of unauthorised access to NSPF's infrastructure or infrastructure of cooperation between the NSPF and the credit institution | Identifier of the order  to transfer funds |
| INN of the credit institution - the recipient of the order |
| No. of recipient's account in the credit institution |
| INN of recipient's credit institution |

STO BR BFBO-1.5-2023

152

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of type (area) of activity of tier one financial institution** | **Name of type (area) of activity of tier one financial institution** | **Code of type (area) of activity of tier two financial institution** | **Name of type (area) of activity of tier two**  **financial institution** | **Code of technological process** | **Name of technological process** | **Code of incident type** | **Code of incident** | **Name of incident** | **Notification criterion** | **Business data of information security incident** |
|  |  | | |  |  | [DT\_FS] | [DT\_FS\_ NGPF\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - non-state pension fund | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - non-state pension fund, | - |
| [DT\_FS\_ NGPF\_2] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution -  non-state pension fund, as well as allowable downtime  and (or) degradation time of the technological process established by the financial institution - non-state pension fund not exceeding  24 hours | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution -  non-state pension fund, as well as allowable downtime  and (or) degradation time of the technological process established by the financial institution - non-state pension fund not exceeding  24 hours | - |
| [placementOfFunds] | Technological process ensuring placement of pension reserve funds | [FM] | [FM\_ NGPF\_4] | Incident related to placement of pension reserve funds as a result of unauthorised access  to NSPF's infrastructure or infrastructure of cooperation between the NSPF and the credit institution | Receiving notification  from a credit institution or unaided identification by the NSPF of the fact of placement of pension reserve funds as a result of unauthorised access to NSPF's infrastructure or infrastructure of cooperation between the NSPF and the credit institution | Identifier of the order  to transfer funds |
| INN of the credit institution - the recipient of the order |
| No. of recipient's account in the credit institution |
| INN of recipient's credit institution |

STO BR BFBO-1.5-2023 153

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of type (area) of activity of tier one financial institution** | **Name of type (area) of activity of tier one financial institution** | **Code of type (area) of activity of tier two financial institution** | **Name of type (area) of activity of tier two**  **financial institution** | **Code of technological process** | **Name of technological process** | **Code of incident type** | **Code of incident** | **Name of incident** | **Notification criterion** | **Business data of information security incident** |
|  |  | | |  |  | [DT\_FS] | [DT\_FS\_ NGPF\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - non-state pension fund | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - non-state pension fund, | - |
| [DT\_FS\_ NGPF\_2] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution -  non-state pension fund, as well as allowable downtime  and (or) degradation time of the technological process established by the financial institution - non-state pension fund not exceeding  24 hours | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution -  non-state pension fund, as well as allowable downtime  and (or) degradation time of the technological process established by the financial institution - non-state pension fund not exceeding  24 hours | - |
| [terminationOfAgreement] | Technological process ensuring termination of a non-state pension provision agreement, statutory pension insurance agreement by a non-state pension fund | [FM] | [FM\_ NGPF\_5] | Incident related to remittance of payments due to termination of the agreement  based on the application of the NSPF's client, generated without its consent, in particular, based on a modified application | Receiving notification from an NSPF's client or unaided  identification by the NSPF of the fact of remittance of payment due to termination of the agreement based on the application of the NSPF's client, generated without its consent, in particular, based on a modified application | Hash of ID or INN of the client (the affected party) |
| Identifier of the order  to transfer funds |

154

STO BR BFBO-1.5-2023

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of type (area) of activity of tier one financial institution** | **Name of type (area) of activity of tier one financial institution** | **Code of type (area) of activity of tier two financial institution** | **Name of type (area) of activity of tier two**  **financial institution** | **Code of technological process** | **Name of technological process** | **Code of incident type** | **Code of incident** | **Name of incident** | **Notification criterion** | **Business data of information security incident** |
|  |  | | |  |  |  |  |  |  | INN of the credit institution - the recipient of the order |
| No. of recipient's account in the credit institution |
| INN of recipient's credit institution |
| [FM\_ NGPF\_6] | Incident related to remittance of payments due to termination of the agreement  as a result of unauthorised access to NSPF's infrastructure or infrastructure of cooperation between the NSPF and the credit institution | Receiving notification  from an NSPF's client or unaided identification by the NSPF of the fact of remittance of payment due to termination of the agreement as a result of unauthorised access to NSPF's infrastructure or infrastructure of cooperation between the NSPF and the credit institution | Hash of ID or INN of the client (the affected party) |
| Identifier of the order  to transfer funds |
| INN of the credit institution - the recipient of the order |
| No. of recipient's account in the credit institution |
| INN of recipient's credit institution |

STO BR BFBO-1.5-2023 155

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of type (area) of activity of tier one financial institution** | **Name of type (area) of activity of tier one financial institution** | **Code of type (area) of activity of tier two financial institution** | **Name of type (area) of activity of tier two**  **financial institution** | **Code of technological process** | **Name of technological process** | **Code of incident type** | **Code of incident** | **Name of incident** | **Notification criterion** | **Business data of information security incident** |
|  |  | | |  |  | [DT\_FS] | [DT\_FS\_ NGPF\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - non-state pension fund | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - non-state pension fund, | - |
| [DT\_FS\_ NGPF\_2] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution -  non-state pension fund, as well as allowable downtime  and (or) degradation time of the technological process established by the financial institution - non-state pension fund not exceeding  24 hours | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution -  non-state pension fund, as well as allowable downtime  and (or) degradation time of the technological process established by the financial institution - non-state pension fund not exceeding  24 hours | - |
| [SIB] | Carrying out activity of insurance entities | | | [accountingOfInsurance] | Technological process ensuring accounting of insured events | [FM] | [FM\_SIB\_1] | Incident related to payment of indemnity based on the application of the client, generated without its consent, in particular, based on a modified application | Receiving notification from a client or unaided identification by an insurance entity of the fact of payment of indemnity based on the application of the client, generated without its consent, in particular, based on a modified application | Hash of ID or INN of the client (the beneficiary) |
| Identifier of the order  to transfer funds |
| INN of the credit institution - the recipient of the order |

156

STO BR BFBO-1.5-2023

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of type (area) of activity of tier one financial institution** | **Name of type (area) of activity of tier one financial institution** | **Code of type (area) of activity of tier two financial institution** | **Name of type (area) of activity of tier two**  **financial institution** | **Code of technological process** | **Name of technological process** | **Code of incident type** | **Code of incident** | **Name of incident** | **Notification criterion** | **Business data of information security incident** |
|  |  | | |  |  |  |  |  |  | No. of recipient's account in the credit institution |
| INN of recipient's credit institution |
| [FM\_SIB\_2] | Incident related to payment of indemnity as a result of unauthorised access to insurance entities' infrastructure | Receiving notification  from a client or unaided identification by an insurance entity of the fact of payment of indemnity as a result of unauthorised access  to insurance entities' infrastructure | Hash of ID or INN of the client |
| Identifier of the order  to transfer funds |
| INN of the credit institution - the recipient of the order |
| No. of recipient's account in the credit institution |
| INN of recipient's credit institution |
| [DT\_FS] | [DT\_FS\_ SIB\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - insurance organisation | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - insurance organisation | - |

STO BR BFBO-1.5-2023 157

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of type (area) of activity of tier one financial institution** | **Name of type (area) of activity of tier one financial institution** | **Code of type (area) of activity of tier two financial institution** | **Name of type (area) of activity of tier two**  **financial institution** | **Code of technological process** | **Name of technological process** | **Code of incident type** | **Code of incident** | **Name of incident** | **Notification criterion** | **Business data of information security incident** |
|  |  | | |  |  |  | [DT\_FS\_ SIB\_2] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - insurance organisation, as well as allowable downtime  and (or) degradation time of the technological process established by the financial institution - insurance organisation  not exceeding 24 hours | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - insurance organisation, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - insurance organisation not exceeding 24 hours | - |
| [refundOfInsurance] | Technological process ensuring refund of insurance premium | [FM] | [FM\_SIB\_3] | Incident related to refund of insurance premium based on the application of the client, generated without its consent, in particular, based on a modified application | Receiving notification from a client or unaided identification by an insurance entity of the fact of refund of insurance premium based on the application of the client, generated without its consent, in particular, based on a modified application | Hash of ID or INN of the client (the beneficiary) |
| Identifier of the order  to transfer funds |
| INN of the credit institution - the recipient of the order |
| No. of recipient's account in the credit institution |
| INN of recipient's credit institution |

158

STO BR BFBO-1.5-2023

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of type (area) of activity of tier one financial institution** | **Name of type (area) of activity of tier one financial institution** | **Code of type (area) of activity of tier two financial institution** | **Name of type (area) of activity of tier two**  **financial institution** | **Code of technological process** | **Name of technological process** | **Code of incident type** | **Code of incident** | **Name of incident** | **Notification criterion** | **Business data of information security incident** |
|  |  | | |  |  |  | [FM\_SIB\_4] | Incident related to refund of insurance premium as a result of unauthorised access to insurance entities' infrastructure | Receiving notification from a client or unaided identification by an insurance entity of the fact of refund of insurance premium as a result of unauthorised access  to insurance entities' infrastructure | Hash of ID or INN of the client |
| Identifier of the order  to transfer funds |
| INN of the credit institution - the recipient of the order |
| No. of recipient's account in the credit institution |
| INN of recipient's credit institution |
| [DT\_FS] | [DT\_FS\_ SIB\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - insurance organisation | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - insurance organisation | - |

STO BR BFBO-1.5-2023 159

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of type (area) of activity of tier one financial institution** | **Name of type (area) of activity of tier one financial institution** | **Code of type (area) of activity of tier two financial institution** | **Name of type (area) of activity of tier two financial institution** | **Code of technological process** | **Name of technological process** | **Code of incident type** | **Code of incident** | **Name of incident** | **Notification criterion** | **Business data of information security incident** |
|  |  | | |  |  |  | [DT\_FS\_ SIB\_2] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - insurance organisation, as well as allowable downtime  and (or) degradation time of the technological process established by the financial institution - insurance organisation  not exceeding 24 hours | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - insurance organisation, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - insurance organisation not exceeding 24 hours | - |
| [maintenanceOfWebsite] | Technological process ensuring operation of websites in respect of placement of information provided for by clause  6 of Article 6 of the Law of the Russian Federation No. 4015-I dated November 27, 1992  "On organisation of insurance activities in the Russian Federation" | [DT\_FS] | [DT\_FS\_ SIB\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - insurance organisation | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - insurance organisation | - |
| [DT\_FS\_ SIB\_2] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - insurance organisation, as well as allowable downtime  and (or) degradation time of the technological process established by the financial institution - insurance organisation  not exceeding 24 hours | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - insurance organisation, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - insurance organisation not exceeding 24 hours | - |

160

STO BR BFBO-1.5-2023

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of type (area) of activity of tier one financial institution** | **Name of type (area) of activity of tier one financial institution** | **Code of type (area) of activity of tier two financial institution** | **Name of type (area) of activity of tier two financial institution** | **Code of technological process** | **Name of technological process** | **Code of incident type** | **Code of incident** | **Name of incident** | **Notification criterion** | **Business data of information security incident** |
| [MFO] | Carrying out activity of microfinance organisations | | | No requirement to notify of the incidents | | | | | | |
| [LCC] | Carrying out activity of consumer credit cooperatives | | | No requirement to notify of the incidents | | | | | | |
| [HCC] | Carrying out activity of housing savings cooperatives | | | No requirement to notify of the incidents | | | | | | |
| [AO] | Carrying out actuarial activity | | | No requirement to notify of the incidents | | | | | | |
| [CRB] | Carrying out activity of credit history bureaus | | | [transferOfSubjectCre ditHistory] | Transfer by the source of credit history of information on the credit history subject to the CHB | [FM] | [FM\_CRB\_1] | Incident related to provision to CHB of information on a credit history subject generated without consent of the source of credit history, in particular, based of a modified credit history of the subject | Identifying by CHB of the fact of provision to CHB of information on a credit history subject generated without consent of the source of credit history, in particular, based of a modified credit history of the subject | No requirement to business data  of information security incident |
| [transferOfSubjectCreditReport] | Transfer by CHB of the subject's credit report to CHB users | [FM] | [FM\_ CRB\_2] | Incident related to transfer by CHB of the modified credit report of the subject  as a result of unauthorised access to CHB's infrastructure | Identification by CHB of the fact of transfer by CHB of the modified credit report of the subject  as a result of unauthorised access to CHB's infrastructure | No requirement to business data  of information security incident |
| [CRA] | Carrying out activity of credit rating agencies | | | No requirement to notify of the incidents | | | | | | |
| [ACCC] | Carrying out activity of agricultural consumer credit cooperatives | | | No requirement to notify of the incidents | | | | | | |
| [PB] | Carrying out activity of pawnshops | | | No requirement to notify of the incidents | | | | | | |
| [OIP] | Carrying out activity of an investment platform operator | | | [accessToPlatform] | Technological process ensuring provision of access to investment platform | [DT\_FS] | [DT\_FS\_ OIP\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - investment platform operator | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - investment platform operator | - |

STO BR BFBO-1.5-2023 161

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of type (area) of activity of tier one financial institution** | **Name of type (area) of activity of tier one financial institution** | **Code of type (area) of activity of tier two financial institution** | **Name of type (area) of activity of tier two financial institution** | **Code of technological process** | **Name of technological process** | **Code of incident type** | **Code of incident** | **Name of incident** | **Notification criterion** | **Business data of information security incident** |
|  |  | | |  |  |  | [DT\_FS\_ OIP\_2] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - investment platform operator, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - investment platform operator not exceeding 24 hours | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - investment platform operator,  as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - investment platform operator not exceeding 24 hours | - |
| [placementOfInvestmentProposal] | Technological process ensuring placement of an investment proposal | [FM] | [FM\_OIP\_1] | Incident related to placement of an investment proposal based on the order of the person attracting investments, generated without its consent, in particular, based on a modified order of the person attracting investments | Receiving notification  from a person attracting investments or unaided identification by the investment platform operator of the fact of placement of an investment proposal based on the order of the person attracting investments, generated without its consent, in particular, based on a modified order of the person attracting investments | No requirement to business data  of information security incident |
| [FM\_OIP\_2] | Incident related to placement of an investment proposal as a result of unauthorised access to investment platform operator's information infrastructure | Receiving notification  from a person attracting investments or unaided identification by the investment platform operator of the fact of placement of an investment proposal as a result of unauthorised access to investment platform operator's information infrastructure | No requirement to business data  of information security incident |

162

STO BR BFBO-1.5-2023

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of type (area) of activity of tier one financial institution** | **Name of type (area) of activity of tier one financial institution** | **Code of type (area) of activity of tier two financial institution** | **Name of type (area) of activity of tier two**  **financial institution** | **Code of technological process** | **Name of technological process** | **Code of incident type** | **Code of incident** | **Name of incident** | **Notification criterion** | **Business data of information security incident** |
|  |  | | |  |  | [DT\_FS] | [DT\_FS\_ OIP\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - investment platform operator | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - investment platform operator | - |
| [DT\_FS\_ OIP\_2] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - investment platform operator, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - investment platform operator not exceeding 24 hours | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - investment platform operator,  as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - investment platform operator not exceeding 24 hours | - |
| [investmentByLoan] | Technological process ensuring investment  using an investment platform through loan extension | [FM] | [FM\_OIP\_3] | Incident related to conclusion of investment agreement based on the investor's request generated without its consent, in particular, based on a modified investor's request | Receiving notification  from an investor or unaided identification by the investment platform operator of the fact of conclusion of investment agreement based on the investor's request generated without its consent, in particular, based on a modified investor's request | No requirement to business data  of information security incident |

STO BR BFBO-1.5-2023 163

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of type (area) of activity of tier one financial institution** | **Name of type (area) of activity of tier one financial institution** | **Code of type (area) of activity of tier two financial institution** | **Name of type (area) of activity of tier two financial institution** | **Code of technological process** | **Name of technological process** | **Code of incident type** | **Code of incident** | **Name of incident** | **Notification criterion** | **Business data of information security incident** |
|  |  | | |  |  |  | [FM\_OIP\_4] | Incident related to conclusion of investment agreement without investor's consent as a result of unauthorised access to the investment platform operator's information infrastructure | Receiving notification  from an investor or unaided identification by the investment platform operator of the fact of conclusion of investment agreement without investor's consent as a result of unauthorised access  to the investment platform operator's information  infrastructure | No requirement to business data  of information security incident |
| [FM\_OIP\_5] | Incident related to conclusion of investment agreement without consent of the person attracting investments as a result of unauthorised access to the investment platform operator's information infrastructure | Receiving notification from the person attracting  investments or unaided identification by the investment platform operator of the fact of conclusion of investment agreement without consent of the person attracting investments as a result of unauthorised access  to the investment platform operator's information infrastructure | No requirement to business data  of information security incident |
| [DT\_FS] | [DT\_FS\_ OIP\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - investment platform operator | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - investment platform operator | - |

164

STO BR BFBO-1.5-2023

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of type (area) of activity of tier one financial institution** | **Name of type (area) of activity of tier one financial institution** | **Code of type (area) of activity of tier two financial institution** | **Name of type (area) of activity of tier two financial institution** | **Code of technological process** | **Name of technological process** | **Code of incident type** | **Code of incident** | **Name of incident** | **Notification criterion** | **Business data of information security incident** |
|  |  | | |  |  |  | [DT\_FS\_ OIP\_2] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - investment platform operator, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - investment platform operator not exceeding 24 hours | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - investment platform operator,  as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - investment platform operator not exceeding 24 hours | - |
| [investmentBySecurities] | Technological process ensuring investment  using an investment platform through purchase of issuable securities placed using the investment platform | [FM] | [FM\_OIP\_3] | Incident related to conclusion of investment agreement based on the investor's request generated without its consent, in particular, based on a modified investor's request | Receiving notification  from an investor or unaided identification by the investment platform operator of the fact of conclusion of investment agreement based on the investor's request generated without its consent, in particular, based on a modified investor's request | No requirement to business data  of information security incident |
| [FM\_OIP\_4] | Incident related to conclusion of investment agreement without investor's consent as a result of unauthorised access to the investment platform operator's information infrastructure | Receiving notification  from an investor or unaided identification by the investment platform operator of the fact of conclusion of investment agreement without investor's consent as a result of unauthorised access  to the investment platform operator's information  infrastructure | No requirement to business data  of information security incident |

STO BR BFBO-1.5-2023 165

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of type (area) of activity of tier one financial institution** | **Name of type (area) of activity of tier one financial institution** | **Code of type (area) of activity of tier two financial institution** | **Name of type (area) of activity of tier two financial institution** | **Code of technological process** | **Name of technological process** | **Code of incident type** | **Code of incident** | **Name of incident** | **Notification criterion** | **Business data of information security incident** |
|  |  | | |  |  |  | [FM\_OIP\_5] | Incident related to conclusion of investment agreement without consent of the person attracting investments as a result of unauthorised access to the investment platform operator's information infrastructure | Receiving notification from the person attracting  investments or unaided identification by the investment platform operator of the fact of conclusion of investment agreement without consent of the person attracting investments as a result of unauthorised access  to the investment platform operator's information infrastructure | No requirement to business data  of information security incident |
| [DT\_FS] | [DT\_FS\_ OIP\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - investment platform operator | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - investment platform operator | - |
| [DT\_FS\_ OIP\_2] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - investment platform operator, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - investment platform operator not exceeding 24 hours | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - investment platform operator,  as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - investment platform operator not exceeding 24 hours | - |

166

STO BR BFBO-1.5-2023

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of type (area) of activity of tier one financial institution** | **Name of type (area) of activity of tier one financial institution** | **Code of type (area) of activity of tier two financial institution** | **Name of type (area) of activity of tier two financial institution** | **Code of technological process** | **Name of technological process** | **Code of incident type** | **Code of incident** | **Name of incident** | **Notification criterion** | **Business data of information security incident** |
|  |  | | | [investmentByUDR] | Technological process ensuring investment  using an investment platform through purchase of utility digital rights | [FM] | [FM\_OIP\_3] | Incident related to conclusion of investment agreement based on the investor's request generated without its consent, in particular, based on a modified investor's request | Receiving notification  from an investor or unaided identification by the investment platform operator of the fact of conclusion of investment agreement based on the investor's request generated without its consent, in particular, based on a modified investor's request | No requirement to business data  of information security incident |
| [FM\_OIP\_4] | Incident related to conclusion of investment agreement without investor's consent as a result of unauthorised access to the investment platform operator's information infrastructure | Receiving notification  from an investor or unaided identification by the investment platform operator of the fact of conclusion of investment agreement without investor's consent as a result of unauthorised access  to the investment platform operator's information  infrastructure | No requirement to business data  of information security incident |
| [FM\_OIP\_5] | Incident related to conclusion of investment agreement without consent of the person attracting investments as a result of unauthorised access to the investment platform operator's information infrastructure | Receiving notification from the person attracting  investments or unaided identification by the investment platform operator of the fact of conclusion of investment agreement without consent of the person attracting investments as a result of unauthorised access  to the investment platform operator's information infrastructure | No requirement to business data  of information security incident |

STO BR BFBO-1.5-2023 167

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of type (area) of activity of tier one financial institution** | **Name of type (area) of activity of tier one financial institution** | **Code of type (area) of activity of tier two financial institution** | **Name of type (area) of activity of tier two financial institution** | **Code of technological process** | **Name of technological process** | **Code of incident type** | **Code of incident** | **Name of incident** | **Notification criterion** | **Business data of information security incident** |
|  |  | | |  |  |  | [FM\_OIP\_6] | Incident related to occurrence, disposal or transfer of utility digital rights as a result of unauthorised access  to the investment platform operator's information infrastructure | Identification by investment platform operator of the fact of occurrence, disposal or transfer of utility digital rights as a result of unauthorised access  to the investment platform operator's information  infrastructure | No requirement to business data  of information security incident |
|  |  | | |  |  | [DT\_FS] | [DT\_FS\_ OIP\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - investment platform operator | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - investment platform operator | - |
| [DT\_FS\_ OIP\_2] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - investment platform operator, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - investment platform operator not exceeding 24 hours | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - investment platform operator,  as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - investment platform operator not exceeding 24 hours | - |
| [investmentByDFA] | Technological process ensuring investment  using an investment platform through purchase of digital financial  assets | [FM] | [FM\_OIP\_3] | Incident related to conclusion of investment agreement based on the investor's request generated without its consent, in particular, based on a modified investor's request | Receiving notification  from an investor or unaided identification by the investment platform operator of the fact of conclusion of investment agreement based on the investor's request generated without its consent, in particular, based on a modified investor's request | No requirement to business data  of information security incident |

168

STO BR BFBO-1.5-2023

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code of type (area) of activity of tier one financial institution | Name of type (area) of activity of tier one financial institution | Code of type (area) of activity of tier two financial institution | Name of type (area) of activity of tier two financial institution | Code of technological process | Name of technological process | Code of incident type | Code of incident | Name of incident | Notification criterion | Business data of information security incident |
|  |  | | |  |  |  | [FM\_OIP\_4] | Incident related to conclusion of investment agreement without investor's consent as a result of unauthorised access to the investment platform operator's information infrastructure | Receiving notification  from an investor or unaided identification by the investment platform operator of the fact of conclusion of investment agreement without investor's consent as a result of unauthorised access  to the investment platform operator's information  infrastructure | No requirement to business data  of information security incident |
| [FM\_OIP\_5] | Incident related to conclusion of investment agreement without consent of the person attracting investments as a result of unauthorised access to the investment platform operator's information infrastructure | Receiving notification from the person attracting  investments or unaided identification by the investment platform operator of the fact of conclusion of investment agreement without consent of the person attracting investments as a result of unauthorised access  to the investment platform operator's information infrastructure | No requirement to business data  of information security incident |
| [FM\_OIP\_7] | Incident related to occurrence, disposal or transfer of digital financial assets as a result of unauthorised access  to the investment platform operator's information infrastructure | Identification by investment platform operator of the fact of occurrence, disposal or transfer of digital financial assets as a result of unauthorised access to the investment platform operator's information infrastructure | No requirement to business data  of information security incident |
| [DT\_FS] | [DT\_FS\_ OIP\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - investment platform operator | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - investment platform operator | - |

STO BR BFBO-1.5-2023 169

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of type (area) of activity of tier one financial institution** | **Name of type (area) of activity of tier one financial institution** | **Code of type (area) of activity of tier two financial institution** | **Name of type (area) of activity of tier two financial institution** | **Code of technological process** | **Name of technological process** | **Code of incident type** | **Code of incident** | **Name of incident** | **Notification criterion** | **Business data of information security incident** |
|  |  | | |  |  |  | [DT\_FS\_ OIP\_2] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - investment platform operator, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - investment platform operator not exceeding 24 hours | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - investment platform operator,  as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - investment platform operator not exceeding 24 hours | - |
| [OFP] | Carrying out activity of financial platform operator | | | [enableMakeTransaction] | Technological process ensuring the possibility for financial platform participants to perform financial transactions using a financial platform | [FM] | [FM\_OFP\_1] | Incident related to transfer of financial services consumer's assets from a special account based on the financial services consumer's demand generated without it consent, in particular, based on a modified financial services consumer's demand | Receiving notification from a financial services consumer or unaided identification by financial platform operator of the fact of transfer of financial services consumer's assets from a special account based on the financial services consumer's demand generated without it consent, in particular, based on a modified financial services consumer's demand | No requirement to business data  of information security incident |
| [FM\_ OFP\_2] | Incident related to transfer of financial services consumer's assets from a special account as a result of unauthorised access to the financial platform operator's information infrastructure | Receiving notification  from a financial services consumer or unaided identification by financial platform operator of the fact of transfer of financial services consumer's assets from a special account as a result of unauthorised access to the financial platform operator's information  infrastructure | No requirement to business data  of information security incident |

170

STO BR BFBO-1.5-2023

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code of type (area) of activity of tier one financial institution | Name of type (area) of activity of tier one financial institution | Code of type (area) of activity of tier two financial institution | Name of type (area) of activity of tier two  financial institution | Code of technological process | Name of technological process | Code of incident type | Code of incident | Name of incident | Notification criterion | Business data of information security incident |
|  |  | | |  |  |  | [FM\_ OFP\_3] | Incident related to performance of financial transactions based on a financial services consumer's request, generated without its consent, in particular, based on a modified financial services consumer's request | Receiving notification from a financial services consumer or unaided identification by financial platform operator of the fact of performance of financial transactions based on a financial services consumer's request, generated without its consent, in particular, based on a modified financial services consumer's request | No requirement to business data  of information security incident |
| [FM\_ OFP\_4] | Incident related to performance of financial transactions as a result of unauthorised access to the financial platform operator's information infrastructure or infrastructure of cooperation between financial services consumer and financial platform | Receiving notification from a financial services consumer or unaided identification by financial platform operator of the fact of performance of financial transactions as a result of unauthorised access to the financial platform operator's information infrastructure or infrastructure of cooperation between financial services consumer and financial platform | No requirement to business data  of information security incident |
| [DT\_FS] | [DT\_FS\_ OFP\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - financial platform operator | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - financial platform operator | - |

STO BR BFBO-1.5-2023 171

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code of type (area) of activity of tier one financial institution | Name of type (area) of activity of tier one financial institution | Code of type (area) of activity of tier two financial institution | Name of type (area) of activity of tier two  financial institution | Code of technological process | Name of technological process | Code of incident type | Code of incident | Name of incident | Notification criterion | Business data of information security incident |
|  |  | | |  |  |  | [DT\_FS\_ OFP\_2] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - financial platform operator, as well as allowable downtime  and (or) degradation time of the technological process established by the financial institution - financial platform operator not exceeding 2 hours for institutions liable to use a standard information security level, for the period exceeding 4 hours for other institutions | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - financial platform operator, as well as allowable downtime  and (or) degradation time of the technological process established by the financial institution - financial platform operator not exceeding 2 hours for institutions liable to use a standard information security level, for the period exceeding 4 hours for other institutions | - |
| [OIDFA] | Operators of information systems  used to issue digital financial assets (DFA) | | | [accessToPlatform] | Technological process ensuring access to information  system, including keeping the register of information system  users | [DT\_FS] | [DT\_FS\_ OIDFA\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution -operator of information system, used to issue digital financial assets | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - operator of information system, used to issue digital financial assets | - |

STO BR BFBO-1.5-2023

172

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code of type (area) of activity of tier one financial institution | Name of type (area) of activity of tier one financial institution | Code of type (area) of activity of tier two financial institution | Name of type (area) of activity of tier two  financial institution | Code of technological process | Name of technological process | Code of incident type | Code of incident | Name of incident | Notification criterion | Business data of information security incident |
|  |  | | |  |  |  | [DT\_FS\_ OIDFA\_2] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - operator of information system, used to issue digital financial assets, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - operator of information system, used to issue digital financial assets not exceeding 6 hours  for institutions liable to use a standard information security level, 12 hours for other institutions | Identification of the fact of exceedance of allowable degradation share of the technological process established by the financial institution - operator of information system, used to issue digital financial assets, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - operator of information system, used to issue digital financial assets not exceeding 6 hours  for institutions liable to use a standard information security level, 12 hours for other institutions | - |
| [issueDFA] | Technological process ensuring issue of digital  financial assets in the information system | [FM] | [FM\_ OIDFA\_1] | Incident related to issue of DFA based on a request on DFA issue generated without consent of the person issuing DFA, in particular, based on a modified request | Receiving notification  from a person issuing DFA or unaided identification by the operator of information system used to issue digital financial assets, the fact of DFA issue based on a request on DFA issue generated without consent of the person issuing DFA, in particular, based on a modified  request | No requirement to business data  of information security incident |

STO BR BFBO-1.5-2023 173

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code of type (area) of activity of tier one financial institution | Name of type (area) of activity of tier one financial institution | Code of type (area) of activity of tier two financial institution | Name of type (area) of activity of tier two  financial institution | Code of technological process | Name of technological process | Code of incident type | Code of incident | Name of incident | Notification criterion | Business data of information security incident |
|  |  | | |  |  |  | [FM\_ OIDFA\_2] | Incident related to DFA issue as a result of unauthorised access to the infrastructure of the operator  of information system used to issue digital financial assets | Identification by the operator of information system used to issue digital financial assets, fact of DFA issue as a result of unauthorised access to the infrastructure of the operator of information system | No requirement to business data  of information security incident |
| [FM\_ OIDFA\_3] | Incident related to DFA issue as a result of use of defects (vulnerabilities) of algorithm(s) ensuring identity of information contained  in all databases forming a distributed register (consensus algorithms) | Identification by the operator of information system used to issue digital financial assets of the fact of DFA issue as a result of use of defects (vulnerabilities) of algorithm(s) ensuring identity of information contained in all databases  forming a distributed register (consensus algorithms) | No requirement to business data  of information security incident |
| [DT\_FS] | [DT\_FS\_ OIDFA\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution -operator of information system, used to issue digital financial assets | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - operator of information system, used to issue digital financial assets | - |

STO BR BFBO-1.5-2023

174

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code of type (area) of activity of tier one financial institution | Name of type (area) of activity of tier one financial institution | Code of type (area) of activity of tier two financial institution | Name of type (area) of activity of tier two  financial institution | Code of technological process | Name of technological process | Code of incident type | Code of incident | Name of incident | Notification criterion | Business data of information security incident |
|  |  | | |  |  |  | [DT\_FS\_ OIDFA\_3] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - operator of information system, used to issue digital financial assets, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - operator of information system, used to issue digital financial assets not exceeding 24 hours | Identification of the fact of exceedance of allowable degradation share of the technological process established by the financial institution - operator of information system, used to issue digital financial assets, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - operator of information system, used to issue digital financial assets not exceeding 24 hours | - |
| [circulationDFA] | Technological process ensuring circulation of digital financial assets in the information system, in particular, redemption of entries on digital financial assets | [FM] | [FM\_ OIDFA\_4] | Incident related to DFA circulation based on the request on DFA circulation generated without consent of DFA holder, in particular,  based on a modified request | Receiving notification from a DFA holder or unaided identification by the operator of information system  used to issue digital financial assets, fact of DFA circulation based on the request on DFA circulation generated without consent of DFA holder,  in particular, based on a modified  request | No requirement to business data  of information security incident |
| [FM\_ OIDFA\_5] | Incident related to DFA circulation as a result of unauthorised access to infrastructure of the operator of information system used to issue digital financial assets | Identification by the operator of information system used to issue digital financial assets, fact of DFA circulation as a result of unauthorised access to the infrastructure of the operator of information system | No requirement to business data  of information security incident |

STO BR BFBO-1.5-2023 175

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code of type (area) of activity of tier one financial institution | Name of type (area) of activity of tier one financial institution | Code of type (area) of activity of tier two financial institution | Name of type (area) of activity of tier two  financial institution | Code of technological process | Name of technological process | Code of incident type | Code of incident | Name of incident | Notification criterion | Business data of information security incident |
|  |  | | |  |  |  | [FM\_  OIDFA\_6] | Incident related to DFA  circulation as a result of use  of defects (vulnerabilities)  of algorithm(s) ensuring  identity  of information contained  in all databases forming  a distributed register  (consensus algorithms) | Identification by the operator of information  system used  to issue  digital financial assets,  fact of DFA circulation as a result  of use of defects  (vulnerabilities) of algorithm(s)  ensuring identity  of information contained  in all databases  forming a distributed  register (consensus algorithms) | No requirement  to business data  of an information security  incident |
| [DT\_FS] | [DT\_FS\_ OIDFA\_1] | Incident related to exceedance of allowable degradation  share of the technological  process established by  the financial institution -  operator of information  system used  to issue digital  financial assets | Identifying the fact of exceedance of allowable degradation share  of the technological process  established by the financial  institution - operator  of information system used  to issue  digital financial assets | - |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

STO BR BFBO-1.5-2023

176

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of type (area) of activity of tier one financial institution** | **Name of type (area) of activity of tier one financial institution** | **Code of type (area) of activity of tier two financial institution** | **Name of type (area) of activity of tier two**  **financial institution** | **Code of technological process** | **Name of technological process** | **Code of incident type** | **Code of incident** | **Name of incident** | **Notification criterion** | **Business data of information security incident** |
|  |  | | |  |  |  | [DT\_FS\_ OIDFA\_2] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - operator of information system, used to issue digital financial assets, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - operator of information system, used to issue digital financial assets not exceeding 6 hours  for institutions liable to use a standard information security level, 12 hours for other institutions | Identification of the fact of exceedance of allowable degradation share of the technological process established by the financial institution - operator of information system, used to issue digital financial assets, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - operator of information system, used to issue digital financial assets not exceeding 6 hours  for institutions liable to use a standard information security level, 12 hours for other institutions | - |
| [accountingDFA] | Technological process ensuring the making of entries by the operator of information system under part 2 of Article 6 of the Federal Law No. 259-FZ dated July 31, 2020  "On digital financial assets, digital currency and introduction of amendments to certain legislative acts of the Russian Federation" | [FM] | [FM\_ OIDFA\_7] | Incident related to making entries in the register of information system operator used to issue digital financial assets as a result of unauthorised access to the operator's infrastructure | Identification by the operator of information systems used to issue digital financial assets, the fact of making entries in the register of information system operator used to issue digital financial assets as a result of unauthorised access  to the operator's infrastructure | No requirement to business data  of information security incident |

STO BR BFBO-1.5-2023 177

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of type (area) of activity of tier one financial institution** | **Name of type (area) of activity of tier one financial institution** | **Code of type (area) of activity of tier two financial institution** | **Name of type (area) of activity of tier two**  **financial institution** | **Code of technological process** | **Name of technological process** | **Code of incident type** | **Code of incident** | **Name of incident** | **Notification criterion** | **Business data of information security incident** |
|  |  | | |  |  | [DT\_FS] | [DT\_FS\_ OIDFA\_1] | Incident related to exceedance of allowable degradation | Identifying the fact of exceedance of allowable degradation share | - |
|  |  | share of the technological | of the technological process |  |
|  |  | process established by | established by the financial |  |
|  |  | the financial institution - | institution - operator |  |
|  |  | operator of information | of information system used |  |
|  |  | system used | to issue |  |
|  |  | to issue digital  financial assets | digital financial assets, |  |
|  | [DT\_FS\_ | Incident related to exceedance | Identifying the fact of exceedance of | - |
|  | OIDFA\_4] | of allowable degradation | allowable degradation share |  |
|  |  | share of the technological process | of the technological process |  |
|  |  | established by the financial | established by the financial |  |
|  |  | institution - operator | institution - operator |  |
|  |  | of information system used | of information system used |  |
|  |  | to issue | to issue |  |
|  |  | digital financial assets | digital financial assets |  |
|  |  | as well as allowable | as well as allowable |  |
|  |  | downtime and (or) degradation time | downtime and (or) degradation time |  |
|  |  | of the technological process | of the technological process |  |
|  |  | established by the financial | established by the financial |  |
|  |  | institution - operator | institution - operator |  |
|  |  | of information system used | of information system used |  |
|  |  | to issue | to issue |  |
|  |  | digital financial assets | digital financial assets |  |
|  |  | not exceeding 2 hours | not exceeding 2 hours |  |
|  |  | for institutions liable | for institutions liable |  |
|  |  | to use a standard information | to use a standard information |  |
|  |  | security level, 4 hours | security level, 4 hours |  |
|  |  | for other institutions | for other institutions |  |

178

STO BR BFBO-1.5-2023

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of type (area) of activity of tier one financial institution** | **Name of type (area) of activity of tier one financial institution** | **Code of type (area) of activity of tier two financial institution** | **Name of type (area) of activity of tier two**  **financial institution** | **Code of technological process** | **Name of technological process** | **Code of incident type** | **Code of incident** | **Name of incident** | **Notification criterion** | **Business data of information security incident** |
|  |  | | | [accountingOfHoldersDFA] | Technological process ensuring the making of accounting entries  in the register of holders of shares of private joint stock companies issuing digital financial assets, certifying rights of participation in the equity of the stated private joint stock companies | [FM] | [FM\_ OIDFA\_8] | Incident related to making accounting entries in the register of holders of shares of private joint stock companies issued in the form of digital financial assets as a result of unauthorised access to infrastructure of the operator of information systems used to issue digital financial assets | Identification by the operator of information systems used to issue digital financial assets, the fact of making accounting entries in the register of holders of shares of private joint stock companies issued in the form of digital financial assets as a result of unauthorised access to infrastructure of the operator of information systems used to issue digital financial assets | No requirement to business data  of information security incident |
| [DT\_FS] | [DT\_FS\_ OIDFA\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution -operator of information system, used to issue digital financial assets | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - operator of information system, used to issue digital financial assets | - |

STO BR BFBO-1.5-2023 179

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of type (area) of activity of tier one financial institution** | **Name of type (area) of activity of tier one financial institution** | **Code of type (area) of activity of tier two financial institution** | **Name of type (area) of activity of tier two**  **financial institution** | **Code of technological process** | **Name of technological process** | **Code of incident type** | **Code of incident** | **Name of incident** | **Notification criterion** | **Business data of information security incident** |
|  |  | | |  |  |  | [DT\_FS\_ OIDFA\_3] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - operator of information system, used to issue digital financial assets, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - operator of information system, used to issue digital financial assets not exceeding 24 hours | Identification of the fact of exceedance of allowable degradation share of the technological process established by the financial institution - operator of information system, used to issue digital financial assets, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - operator of information system, used to issue digital financial assets not exceeding 24 hours | - |
| [interactionWithOEDFA] | Technological process ensuring cooperation with the digital financial assets exchange operator | [DT\_FS] | [DT\_FS\_ OIDFA\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution -operator of information system, used to issue digital financial assets | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - operator of information system, used to issue digital financial assets | - |

180

STO BR BFBO-1.5-2023

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of type (area) of activity of tier one financial institution** | **Name of type (area) of activity of tier one financial institution** | **Code of type (area) of activity of tier two financial institution** | **Name of type (area) of activity of tier two**  **financial institution** | **Code of technological process** | **Name of technological process** | **Code of incident type** | **Code of incident** | **Name of incident** | **Notification criterion** | **Business data of information security incident** |
|  |  | | |  |  |  | [DT\_FS\_ OIDFA\_2] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - operator of information system, used to issue digital financial assets, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - operator of information system, used to issue digital financial assets not exceeding 6 hours  for institutions liable to use a standard information security level, 12 hours for other institutions | Identification of the fact of exceedance of allowable degradation share of the technological process established by the financial institution - operator of information system, used to issue digital financial assets, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - operator of information system, used to issue digital financial assets not exceeding 6 hours  for institutions liable to use a standard information security level, 12 hours for other institutions | - |
| [monitoringOfImmutability] | Technological process ensuring monitoring of identity of information contained in all databases forming a distributed register | [DT\_FS] | [DT\_FS\_ OIDFA\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution -operator of information system, used to issue digital financial assets | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - operator of information system, used to issue digital financial assets | - |

STO BR BFBO-1.5-2023 181

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of type (area) of activity of tier one financial institution** | **Name of type (area) of activity of tier one financial institution** | **Code of type (area) of activity of tier two financial institution** | **Name of type (area) of activity of tier two**  **financial institution** | **Code of technological process** | **Name of technological process** | **Code of incident type** | **Code of incident** | **Name of incident** | **Notification criterion** | **Business data of information security incident** |
|  |  | | |  |  |  | [DT\_FS\_ OIDFA\_2] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - operator of information system, used to issue digital financial assets, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - operator of information system, used to issue digital financial assets not exceeding 6 hours  for institutions liable to use a standard information security level, 12 hours for other institutions | Identification of the fact of exceedance of allowable degradation share of the technological process established by the financial institution - operator of information system, used to issue digital financial assets, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - operator of information system, used to issue digital financial assets not exceeding 6 hours  for institutions liable to use a standard information security level, 12 hours for other institutions | - |
| [OEDFA] | Digital financial assets (DFA) exchange operators | | | [enableDealsWithDFA] | Technological process ensuring the possibility of performance of transactions with digital financial assets | [FM] | [FM\_ OEDFA\_1] | Incident related to performance of transactions with digital financial assets based on a DFA exchange request generated without consent of the person exchanging DFA, in particular, based on a modified request | Receiving notification  from a person exchanging DFA or unaided identification by the digital financial assets exchange operator of the fact of performance of transaction with digital financial assets based on a DFA exchange request generated without consent of the person exchanging  DFA, in particular, based on a modified request | No requirement to business data  of information security incident |

182

STO BR BFBO-1.5-2023

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of type (area) of activity of tier one financial institution** | **Name of type (area) of activity of tier one financial institution** | **Code of type (area) of activity of tier two financial institution** | **Name of type (area) of activity of tier two**  **financial institution** | **Code of technological process** | **Name of technological process** | **Code of incident type** | **Code of incident** | **Name of incident** | **Notification criterion** | **Business data of information security incident** |
|  |  | | |  |  |  | [FM\_ OEDFA\_2] | Incident related to performance of transactions with digital financial assets as a result of unauthorised access to infrastructure of digital financial assets exchange operator or infrastructure of cooperation between the person exchanging DFA  and information system used to exchange digital financial assets | Receiving notification  from a person exchanging DFA or unaided identification by the digital financial assets exchange operator of the fact of performance of transaction with digital financial assets  as a result of unauthorised access to infrastructure of digital financial assets exchange operator or infrastructure of cooperation between the person exchanging DFA and information system used  to exchange digital financial assets | No requirement to business data  of information security incident |
| [FM\_ OEDFA\_3] | Incident related to performance of transactions with digital financial assets as a result of use of defects (vulnerabilities) of algorithm(s)  ensuring identity of information contained in all databases forming a distributed register | Unaided identification by the digital financial assets exchange operator of the fact of performance of transaction with digital financial assets  as a result of use of defects (vulnerabilities) of algorithm(s) ensuring identity of information contained in all databases forming a distributed register (consensus  algorithms) | No requirement to business data  of information security incident |
| [FM\_ OEDFA\_4] | Incident related to transfer of digital financial assets to a digital wallet other than DFA recipient's digital wallet as a result of unauthorised access to infrastructure of digital financial assets exchange operator | Receiving notification from a DFA recipient or unaided identification by the digital financial assets exchange operator of the fact of transfer of DFA  to a digital wallet other than DFA recipient's digital  wallet | No requirement to business data  of information security incident |

STO BR BFBO-1.5-2023 183

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of type (area) of activity of tier one financial institution** | **Name of type (area) of activity of tier one financial institution** | **Code of type (area) of activity of tier two financial institution** | **Name of type (area) of activity of tier two**  **financial institution** | **Code of technological process** | **Name of technological process** | **Code of incident type** | **Code of incident** | **Name of incident** | **Notification criterion** | **Business data of information security incident** |
|  |  | | |  |  | [DT\_FS] | [DT\_FS\_ OEDFA\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - digital financial assets exchange operator | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - digital financial assets exchange operator | - |
| [DT\_FS\_ OEDFA\_2] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - digital financial assets exchange operator, as well as allowable downtime  and (or) degradation time of the technological process established by the financial institution - digital financial assets exchange operator, not exceeding 6 hours for institutions liable to use a standard information security level, 12 hours for other institutions | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - digital financial assets exchange operator, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - digital financial assets exchange operator, not exceeding  6 hours for institutions liable to use a standard information security level, 12 hours for other institutions | - |
| [interactionWithOIDFA] | Technological process ensuring cooperation with information system operator | [DT\_FS] | [DT\_FS\_ OEDFA\_1] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - digital financial assets exchange operator | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - digital financial assets exchange operator | - |

184

STO BR BFBO-1.5-2023

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of type (area) of activity of tier one financial institution** | **Name of type (area) of activity of tier one financial institution** | **Code of type (area) of activity of tier two financial institution** | **Name of type (area) of activity of tier two**  **financial institution** | **Code of technological process** | **Name of technological process** | **Code of incident type** | **Code of incident** | **Name of incident** | **Notification criterion** | **Business data of information security incident** |
|  |  | | |  |  |  | [DT\_FS\_ OEDFA\_2] | Incident related to exceedance of allowable degradation share of the technological process established by the financial institution - digital financial assets exchange operator, as well as allowable downtime  and (or) degradation time of the technological process established by the financial institution - digital financial assets exchange operator, not exceeding 6 hours for institutions liable to use a standard information security level, 12 hours for other institutions | Identifying the fact of exceedance of allowable degradation share of the technological process established by the financial institution - digital financial assets exchange operator, as well as allowable downtime and (or) degradation time of the technological process established by the financial institution - digital financial assets exchange operator, not exceeding  6 hours for institutions liable to use a standard information security level, 12 hours for other institutions | - |

APPENDIX 12. DATA PROVISION FORM NTF\_ISI\_DETECT – FORM OF PROVISION BY INFORMATION EXCHANGE PARTICIPANTS OF DATA

ABOUT IDENTIFICATION OF AN INFORMATION SECURITY INCIDENT

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 1 | Type of notification | Type of notification | O | - | [NTF\_ISI\_Detect] | Pre-filled field |
| 2 | Date and time | Date and time of identification of an information security incident | O | - | In accordance with RFC 3339 | Moscow time [UTC +03:00] |
| 3 | Classification  of an information security  incident | Code of type (area)  of activity  of financial  institution | O | - | Selection of one value  from the list:  From the classifier  "Classifier  of information security  and  operational reliability  incidents  broken down by  activities of credit  institutions,  non-banking financial  institutions  and national payment  system  subjects and their constituent  technological  processes"  set forth  in [Appendix 11](#_bookmark31) | If a code  of the type (area)  of activity of tier  one and two  financial institution  is available, they shall be  specified using ".",  for instance: [Code 1].  [Code 2] |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| 4 | Code of technological process | O | - | Selection of one value from the list:  From the classifier  "Classifier  of information security  and  operational reliability  incidents  broken down by  activities of credit  institutions,  non-banking financial  institutions  and national payment  system  subjects and their constituent  technological  processes"  set forth  in [Appendix 11](#_bookmark31)  The list depends  on the field "Code of type  (area) of activity  of financial  institution" | - |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| 5 |  | Code of risk source | O | - | Selection of one value from the list:  From the classifier  "Risk sources"  set forth  in [Appendix 28](#_bookmark67) | - |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 6 |  | Code of incident type | O | - | Selection of one value from the list:  From the classifier  "Classifier of information security and operational reliability incidents broken down by activities of credit  institutions, non-banking financial institutions and national payment system subjects and their constituent technological processes set forth  in [Appendix 11](#_bookmark31)  The list depends  on the field "Code of technological  process' | - |
| 7 | Code of incident | O | - | Selection of one value from the list:  From the classifier  "Classifier of information security and operational reliability incidents broken down by activities of credit  institutions, non-banking financial institutions and national payment system subjects and their constituent technological processes set forth  in [Appendix 11](#_bookmark31)  The list depends on the field "Code of type of information security incident" | - |
| 8 | Business data of financial incident | Dataset  depending on the incident | CO | "Code of type of financial incident" = [FM] and business data are to be filled in | From the classifier  "Classifier of information security and operational reliability incidents broken down by activities of credit  institutions, non-banking financial institutions and national payment system subjects and their constituent technological processes set forth  in [Appendix 11](#_bookmark31) | The structure of data depends on the "Code of information security incident" |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 9 |  | Type of asset |  |  | Text field | - |
| 10 | Number of assets | Integer number >0 | - |
| 11 | Value of single asset | Amount in rubles  accurate to two  decimal places | - |
| 12 | Device digital footprint | Device digital footprint obtained in accordance  with the recommendations of the Bank of Russia | To be filled in, where it is technically feasible to obtain the device digital footprint used to perform the financial operation |
| 13 | Relation to other notifications | Type of related notification | CO | To be filled in, where the Bank of Russia was previously  sent the notification related to the current notification | Selection of one value from the list:  [NTF\_OWC] [NTF\_ISI] [NTF\_ORI] [NTF\_CI] [NTF\_CA] [NTF\_VLN] | [NTF\_OWC] - notification  about identified cases and (or) attempts of  funds transfers without consent of the client as well as  identified cases (or attempts) of carrying out of operations aimed at consummation of financial transactions using financial platform, not relying on the financial platform participant's will [NTF\_ISI] - notification about identification of an information security incident or the findings of investigation of an information security incident [NTF\_ORI] - notification about identification of an operational reliability incident or the findings of investigation of an operational reliability incident  [NTF\_CI] - notification about computer incidents  [NTF\_CA] - notification about computer attacks  [NTF\_VLN] - notification about identified  vulnerabilities |
| 14 |  | Type of relation to other notifications |  |  | Selection of one value from the list: | - |
|  |  |  |  |  | [Preceding event]  [Subsidiary event] [Related event] [Specification of information  about event] |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 15 |  | Registration number of notification |  |  | In accordance  with AIPS FinTsERT format | Identifier of notification or response to the request previously sent  to FinTsERT by an information exchange  participant |
| 16 | Restrictive TLP marker | Restrictive marker for distribution of information from the given notification | N | - | Selection of one value from the list:  [TLP: WHITE] [TLP: GREEN] [TLP: AMBER] [TLP: RED] | In accordance  with designations accepted in TLP protocol  Default value [TLP: GREEN], unless otherwise specified |
| 17 | Necessity of FinTsERT involvement | Necessity of FinTsERT involvement | CO | Where necessary | [Yes] | Necessity to engage FinTsERT to investigate the information security incident, the findings whereof shall be sent in the investigation notice |

APPENDIX 13. DATA PROVISION FORM NTF\_ISI\_DATALEAK – FORM OF PROVISION BY INFORMATION EXCHANGE PARTICIPANTS OF DATA

ABOUT IDENTIFICATION OF UNLAWFUL DISCLOSURE OF BANK SECRET AND (OR)

PROTECTED INFORMATION UNDER REGULATORY ACTS OF THE BANK OF RUSSIA

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 1 | Type of notification | Type of notification | O | - | [NTF\_ISI\_DataLeak] | Pre-filled field |
| 2 | Date and time | Date of identification of the fact of unlawful disclosure of bank secret, personal data and (or) other data of clients or employees of an information exchange participant | O | - | In accordance with RFC 3339 | Moscow time [UTC +03:00] |
| 3 | General information  about the fact of unlawful disclosure of information | Type of unlawfully disclosed information | O | - | [Bank secret] [Personal data]  [Other protected  information] | - |
| 4 | Supposed reasons of unlawful disclosure of information | O | - | Text field | Description of events having resulted  in unlawful disclosure  of information |
| 5 | Supposed damage caused to the subjects' rights | O | - | Text field | Description of supposed damage which may be caused to the subjects upon use of unlawfully disclosed information |
| 6 | Characteristics of unlawfully disclosed information | Type of subject whose information was disclosed | O | - | [Employee] [Client] [Partner] [Other] | [Employee] - Employees of financial institution [Client] - Clients  of financial institution  [Partner] - Partners, counterparties, contractors etc. of financial institution  [Other] - Other |
| 7 | Structure of unlawfully disclosed information | O | - | Text field | Description of data structure of unlawfully disclosed information |
| 8 | Number of entries of unlawfully disclosed information | CO | Where the extent of unlawfully disclosed information may be measured based on the number of entries (for instance, DB lines) | Number | Actual or supposed number of entries |
| 9 | Relevance of unlawfully disclosed information | O | - | [Data are relevant] [Data are irrelevant] | - |
| 10 | Information about a person authorised by the operator  to interact with Roskomnadzor  on the incident | Full name of the person authorised by the operator to interact  with Roskomnadzor on the incident | CO | "Type of unlawfully disclosed information"  = [Personal data] | Text field | - |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 11 |  | Mobile telephone of the person authorised to interact with Roskomnadzor on the incident |  |  | In accordance with the Russian numbering system  and plan | - |
| 12 | E-mail address for sending information about notification | In the format  of e-mail address | - |
| 13 | Relation to other notifications | Type of related notification | CO | To be filled in, where the Bank of Russia was previously  sent the notification related to the current notification | [NTF\_OWC] [NTF\_ISI] [NTF\_ORI] [NTF\_CI] [NTF\_CA] [NTF\_VLN] | [NTF\_OWC] - notification  about identified cases and (or) attempts of  funds transfers without consent of the client as well as  identified cases (or attempts) of carrying out of operations aimed at consummation of financial transactions using financial platform, not relying on the financial platform participant's will [NTF\_ISI] - notification about identification of an information security incident or the findings of investigation of an information security incident [NTF\_ORI] - notification about identification of an operational reliability incident or the findings of investigation of an operational reliability incident  [NTF\_CI] - notification about computer incidents  [NTF\_CA] - notification about computer attacks  [NTF\_VLN] - notification about identified  vulnerabilities |
| 14 | Type of relation to other notifications | [Preceding event]  [Subsidiary event] [Related event] [Specification of information  about event] | - |
| 15 | Registration number of notification | In accordance  with AIPS FinTsERT format | Identifier of notification or response to the request previously sent  to FinTsERT by an information exchange  participant |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 16 | Restrictive TLP marker | Restrictive marker for distribution of information from the given notification | N | - | Selection of one value from the list:  [TLP: WHITE] [TLP: GREEN] [TLP: AMBER] [TLP: RED] | In accordance  with designations accepted in TLP protocol.  Default value [TLP: GREEN], unless otherwise specified |
| 17 | Necessity of FinTsERT involvement | Necessity of FinTsERT involvement | CO | Where necessary | [Yes] | Necessity to engage FinTsERT to investigate unlawful disclosure of information, the findings whereof shall be sent in the investigation notice |

APPENDIX 14. DATA PROVISION FORM NTF\_ISI\_INVESTIGATION – FORM OF PROVISION BY INFORMATION EXCHANGE PARTICIPANTS

OF DATA ABOUT THE FINDINGS OF INVESTIGATION OF AN INFORMATION SECURITY INCIDENT OR UNLAWFUL DISCLOSURE OF BANK SECRET AND (OR) PROTECTED

INFORMATION UNDER REGULATORY ACTS OF THE BANK OF RUSSIA

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 1 | Type of notification | Type of notification | O | - | [NTF\_ISI\_Investigation] | Pre-filled field |
| 2 | Relation to notification about identification of an information security incident or unlawful disclosure of bank secret, personal data and (or) other data of clients and employees of an information exchange participant | Identifier(s) of notification about identification of an information security incident or unlawful disclosure of bank secret, personal data and (or) other data of clients and employees of an information exchange participant | O | - | In accordance  AIPS FinTsERT format.  Where several identifiers are specified, they are to be enumerated using  ";' | Identifier of notification or response to the request previously sent  to FinTsERT by an information exchange participant.  Where the notification about the findings of investigation describes the attack scenario having resulted in several information security incidents or events of unlawful disclosure of bank secret, personal data and (or) other data of clients or employees of an information exchange participant, all related notifications about identification of an information security incident or unlawful disclosure of bank secret, personal data and (or) other data of clients or employees of an information exchange participant are to be specified |
| 3 | Date and time | Date and time of actual occurrence of an information security incident | O | - | In accordance with RFC 3339 | Moscow time [UTC +03:00] |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 4 | Specification of data  contained  in the notification about  identification of information  security incident | Code of type (area)  of activity  of financial  institution | CO | Where necessary  to specify classification  of information  security incident,  previously provided  in the notification  about identification  of an information security  incident | Selection of one value  from the list:  From the classifier  "Classifier  of information security  and  operational reliability  incidents  broken down by  activities of credit  institutions,  non-banking financial  institutions  and national payment  system  subjects and their constituent  technological  processes"  set forth  in [Appendix 11](#_bookmark31) | If a code  of the type (area)  of activity of tier  one and two  financial institution  is available, they shall be  specified using ".",  for instance: [Code 1].  [Code 2] |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |  |
| 5 | Code of technological process |  | Selection of one value from the list: | - |
|  |  |  | From the classifier |  |
|  |  |  | "Classifier |  |
|  |  |  | of information security |  |
|  |  |  | and |  |
|  |  |  | operational reliability |  |
|  |  |  | incidents |  |
|  |  |  | broken down by |  |
|  |  |  | activities of credit |  |
|  |  |  | institutions, |  |
|  |  |  | non-banking financial |  |
|  |  |  | institutions |  |
|  |  |  | and national payment |  |
|  |  |  | system |  |
|  |  |  | subjects and their constituent |  |
|  |  |  | technological |  |
|  |  |  | processes" |  |
|  |  |  | set forth |  |
|  |  |  | in [Appendix 11](#_bookmark31) |  |
|  |  |  | The list depends |  |
|  |  |  | on the field "Code of type |  |
|  |  |  | (area) of activity |  |
|  |  |  | of financial |  |
|  |  |  | institution" |  |
| 6 | Code of risk source |  | Selection of one value from the list: | - |
|  |  |  | From the classifier |  |
|  |  |  | "Risk sources" |  |
|  |  |  | set forth |  |
|  |  |  | in [Appendix 28](#_bookmark67) |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 7 |  | Code of incident type |  |  | Selection of one value from the list:  From the classifier  "Classifier of information security and operational reliability incidents broken down by activities of credit  institutions, non-banking financial institutions and national payment system subjects and their constituent technological processes set forth  in [Appendix 11](#_bookmark31)  The list depends  on the field "Code of technological  process' | - |
| 8 | Code of incident | Selection of one value from the list:  From the classifier  "Classifier of information security and operational reliability incidents broken down by activities of credit  institutions, non-banking financial institutions and national payment system subjects and their constituent technological processes set forth  in [Appendix 11](#_bookmark31)  The list depends on the field "Code of type of information security incident" | - |
| 9 | Attack scenario | Attack scenario | CO | At least one of the fields must be filled in | In the format: {ID of tactic 1}. {ID of technique 1}: {ID of tactic 2}. {ID of technique 2} + {ID of technique 3}: {ID of tactic 3}.  {ID of technique 4} | Successive list of identifiers of techniques  and tactics of an attack based on MITRE  ATT&CK matrix |
| 10 | Description of attack scenario | Text field | Textual description of attack scenario. To be filled in, where MITRE  ATT&CK matrix lacks the necessary  techniques/tactics |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 11 | Attack template (to be filled in separately for each tactic  of "Attack scenario") | Identifier of tactic | O | - | In the format: {ID of tactic}. {ID of technique} or text field | Identifier of tactic being the constituent part  of "Attack scenario" or attack step  from "Description of attack  scenario" |
| 12 | Procedure | O | - | Text field | Description of the procedure reflecting tactic implementation |
| 13 | Name of technological site where the tactic is implemented | O | - | Selection of one value from the list:  From the classifier  "Technological sites" set forth in [Appendix](#_bookmark67)  [28](#_bookmark67) | - |
| 14 | Code of level of object/subject being the target  of attack | O | - | Selection of one value from the list:  From the classifier  "Types of objects and subjects" set forth  in [Appendix 28](#_bookmark67) | The block is to be filled in separately for each object/subject, being the target of attack |
| 15 | Code of type of object/subject being the target  of attack | O | - | "Selection of one value from the list:  From the classifier  "Types of objects and subjects" set forth  in [Appendix 28](#_bookmark67)  The list depends on the field "Code of level of object/subject" |
| 16 | Description of information infrastructure facility being the target of attack in CPE format | CO | "Code of level of object/subject" ≠ [Subject] | In the format consistent with the recommendations of the Bank of Russia published on the official website |
| 17 | Identifier of attack | CO | The procedure corresponds to attack of CAPEC classifier | From CAPEC classifier | Identifier of CAPEC attack corresponding to the procedure |
| 18 | List of used security weaknesses in the process of attack | CO | In the course of investigation use of security weaknesses has been identified | Text field  Where several security weaknesses are used, they are specified using  "+" | List of used security weaknesses of software and hardware in the selected system of description of security weaknesses |
| 19 | Name of system of description of security weaknesses | Selection of one value from the list:  [CWE]  [TDB FSTEC] |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 20 |  | List of used security vulnerabilities in the process of attack | CO | In the course of investigation use of security vulnerabilities has been identified | Text field  Where several security vulnerabilities are used, they are specified using  "+" | List of used security vulnerabilities of software and hardware in the selected system of description of security vulnerabilities |
| 21 | Name of system of description of security vulnerabilities | Selection of one value from the list:  [CVE]  [TDB FSTEC] |
| 22 | Software used by the attacked | N | - | Text field | In case of availability of respective information |
| 23 | Indicators of compromise | CO | Where in the process of investigation indicators of compromise have been identified which were not previously sent to FinTsERT | Text field or file | - |
| 24 | Adopted measures | Adopted counter measures | CO | At least one of the fields must be filled in | List of indicators of counter measures | List of indicators of counter measures aimed  at neutralisation of attack and avoidance of repeated attacks  based on MITRE  DEF3ND matrix |
| 25 | Description of protection measures | Text field | Textual description of adopted measures for neutralisation of attack and avoidance of repeated attacks |
| 26 | Damage from the incident | Amount of direct losses | CO | If such losses are consequences of financial incident materialisation and where there is a possibility of their assessment | Amount in rubles  accurate to two decimal places | Direct losses of a financial organisation include losses reported in bookkeeping accounts of expenses and losses  and similar  accounts reflecting  receivables |
| 27 | Amount of indirect losses | CO | If such losses are consequences of financial incident materialisation and where there is a possibility of their assessment | Amount in rubles  accurate to two decimal places | Indirect losses of a financial institution not reported in accounting but indirectly related to information security threat risk events including losses determined through calculation method in monetary terms |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 28 |  | Qualitative losses | CO | Where an institution is subject to requirements on assessment of such losses under 716-P | [Very high] [High] [Medium] [Low] | Indirect losses of a financial institution not reported in accounting but indirectly related to information security threat risk events including losses determined based on expert opinion, where losses are not expressed in monetary terms through calculation method |
| 29 | Amount of potential losses | CO | If such losses are consequences of financial incident materialisation and where there is a possibility of their assessment | Amount in rubles  accurate to two decimal places | Indirect losses of a financial institution not reported in accounting but indirectly related to information security threat risk events including losses having not resulted in direct or indirect losses which could have arise upon realisation  of information security threat risk sources not identified by the financial institution and (or) upon unfavorable coincidence of circumstances |
| 30 | Measures taken by the credit institution for the purposes of receiving indemnity against incurred losses | CO | Where such measures were/are taken | Text field | - |
| 31 | Unique sequential identification number of an operational risk event | Unique sequential identification number of an operational risk event in the database of events corresponding to the given incident | CO | Only for credit institutions | Text field | - |

APPENDIX 15. DATA PROVISION FORM REQ\_ISI\_DATALEAK - FORM OF THE BANK OF RUSSIA'S REQUEST FOR THE PURPOSES OF ACKNOWLEDGING THE FACT OF UNLAWFUL

DISCLOSURE OF BANK SECRET AND (OR) PROTECTED INFORMATION UNDER REGULATORY ACTS OF THE BANK OF RUSSIA

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 1 | Type of request/response | Type of request/response | O | - | [REQ\_ISI\_DataLeak] | Pre-filled field |
| 2 | General information of the request | Type of unlawfully disclosed information | O | - | [Bank secret] [Personal | - |
|  |  |  |  |  | data] |  |
|  |  |  |  |  | [Other protected |  |
|  |  |  |  |  | information] |  |
| 3 |  | Description of unlawfully | O | - | Text field | - |
|  |  | disclosed |  |  |  |  |
|  |  | information |  |  |  |  |
| 4 |  | Date of identification | O | - | In accordance with RFC 3339 | Moscow time [UTC +03:00] |
| 5 |  | Reference to announcement | CO | In case of availability of | Text field | - |
|  |  | based on disclosed |  |  |  |  |
|  |  | information |  |  |  |  |

### Data provision form RESP\_ISI\_DataLeak - Form of submission of response to request of the Bank of Russia for the purposes of acknowledging the fact of unlawful disclosure of bank secret and (or) protected information under regulatory acts of the Bank of Russia

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 1 | Type of request/response | Type of request/response | O | - | [RESP\_ISI\_DataLeak] | Pre-filled field |
| 2 | Status | Status of identification  of unlawful disclosure  of bank  secret, personal  data and (or) other  data of clients or  employees of an information  exchange  participant | O | - | [Fact of unlawful  disclosure has been identified,  information was previously  submitted to the Bank  of Russia]  [Fact of unlawful  disclosure has not been  identified]  [Additional time  for consideration is  required] | - |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| 3 | Identifier of related notification | Identifier of notification about identification of unlawful disclosure of bank  secret, personal  data and (or) other  data of clients or  employees of an information  exchange  participants | CO | "Status" = [Yes, information was previously  submitted to the Bank  of Russia] | In accordance  with AIPS FinTsERT  format | Identifier of notification about identification of unlawful disclosure  of bank  secret, personal  data and (or) other  data of clients or  employees of an information  exchange  participant, previously  sent  to FinTsERT by an information  exchange  participant |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |  |

APPENDIX 16. DATA PROVISION FORM NTF\_ORI\_DETECT – FORM OF PROVISION BY INFORMATION EXCHANGE PARTICIPANTS OF DATA

ABOUT IDENTIFICATION OF AN OPERATIONAL RELIABILITY INCIDENT

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 1 | Type of notification | Type of notification | O | - | [NTF\_ORI\_Detect] | Pre-filled field |
| 2 | Date and time | Date and time of identification of an operational reliability incident | O | - | In accordance with RFC 3339 | Moscow time [UTC +03:00] |
| 3 | Classification of operational reliability incident | Code of type (area) of activity of financial institution | O | - | Selection of one value from the list:  From the classifier  "Classifier of information security and operational reliability incidents broken down by activities of credit  institutions, non-banking financial institutions and national payment system subjects and their constituent technological processes set forth  in [Appendix 11](#_bookmark31) | If a code of type (area) of activity of tier one and two financial institution is available, they shall be specified using ".", for instance: [Code 1].  [Code 2] |
| 4 |  | Code of technological process | O | - | Selection of one value from the list: | - |
|  |  |  |  |  | From the classifier  "Classifier of information security and operational reliability incidents broken down by activities of credit  institutions, non-banking financial institutions and national payment system subjects and their constituent technological processes set forth  in [Appendix 11](#_bookmark31) |  |
|  |  |  |  |  | The list depends on the field "Code of type (area) of activity of financial institution" |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 5 |  | Code of risk source | O | - | Selection of one value from the list: | - |
|  |  |  |  | From the classifier |  |
|  |  |  |  | "Risk sources" |  |
|  |  |  |  | set forth |  |
|  |  |  |  | in [Appendix 28](#_bookmark67) |  |
| 6 | Code of incident type | O | - | Selection of one value from the list:  From the classifier  "Classifier  of information security  and  operational reliability  incidents  broken down by  activities of credit  institutions,  non-banking financial  institutions  and national payment  system  subjects and their constituent  technological  processes"  set forth  in [Appendix 11](#_bookmark31)  The list depends  on the field "Code of technological  process' | - |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| 7 | Code of incident | O | - | Selection of one value from the list:  From the classifier  "Classifier  of information security  and  operational reliability  incidents  broken down by  activities of credit  institutions,  non-banking financial  institutions  and national payment  system  subjects and their constituent  technological  processes"  set forth  in [Appendix 11](#_bookmark31)  The list depends  on the field "Code of type  of an information security  incident" | - |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 8 | Information about information  infrastructure  facility  (The block is to be filled in separately  for each  information  infrastructure  facility having  affected downtime  or degradation  of technological  process) | Code of level | O | - | Selection of one value  from the list:  From the classifier  "Types of objects  and subjects"  set forth  in [Appendix 28](#_bookmark67) | - |
|  | of information infrastructure |  |  |  |
|  | facility |  |  |  |
|  | having |  |  |  |
|  | affected downtime |  |  |  |
|  | or degradation |  |  |  |
|  | of technological |  |  |  |
|  | process |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| 9 | Code of type of information  infrastructure  facility  having  affected downtime  or degradation  of technological  process | O | - | Selection of one value | - |
|  |  |  |  | from the list: |  |
|  |  |  |  |  |  |
|  |  |  |  | From the classifier |  |
|  |  |  |  | "Types of objects |  |
|  |  |  |  | and subjects" |  |
|  |  |  |  | set forth |  |
|  |  |  |  | in [Appendix 28](#_bookmark67) |  |
|  |  |  |  | The list depends |  |
|  |  |  |  | on the field "Code of level of |  |
|  |  |  |  | information |  |
|  |  |  |  | infrastructure |  |
|  |  |  |  | facility" |  |
| 10 |  | Description of information  infrastructure  facility  having affected  downtime or  degradation of technological  process  in CPE format | O | - | In the format corresponding | - |
|  |  |  |  | to the recommendations |  |
|  |  |  |  | of the Bank of Russia |  |
|  |  |  |  | published |  |
|  |  |  |  | on the official |  |
|  |  |  |  | website |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| 11 | Information about an operational reliability incident | Services provision regime established by the institution | O | - | Specified in the format {days\*hours} a quarter | Total number of days  and total number of hours in the reporting quarter of occurrence of the operational reliability incident are specified assessed  in accordance  with the services  provision regime established in the  institution |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 12 | Relation to other notifications | Type of related notification | CO | To be filled in, where the Bank of Russia was previously  sent  a notification related  to the current notification | Selection of one value from the list:  [NTF\_OWC]  [NTF\_ISI]  [NTF\_ORI]  [NTF\_CI]  [NTF\_CA]  [NTF\_VLN] | [NTF\_OWC] - notification  about identified  cases  and (or) attempts  of funds  transfers  without consent  of the client as well as  identified cases  and (or attempts)  of carrying out of  operations aimed  at consummation  of financial  transactions using  financial  platform, not relying on  the financial  platform  participant's will  [NTF\_ISI] - notification  about identification  of an information security  incident or  the findings of investigation  of an information  security incident  [NTF\_ORI] - notification  about identification  of an operational  reliability incident  or the findings  of investigation of an operational  reliability  incident  [NTF\_CI] - notification  about computer  incidents  [NTF\_CA] - notification  about computer  attacks  [NTF\_VLN] - notification  about identified  vulnerabilities" |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| 13 | Type of relation to other notifications |  |  | Selection of one value from the list:  [Preceding  event]  [Subsidiary event]  [Related event]  [Specification of information  about event] | - |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| 14 | Registration number of notification |  |  | In accordance  with AIPS FinTsERT  format | Identifier of notification or response to the request  previously sent  to FinTsERT by an information  exchange  participant |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| 15 | Restrictive TLP marker | Restrictive marker for distribution of information from the given notification | N | - | Selection of one value from the list:  [TLP: WHITE] [TLP: GREEN] [TLP: AMBER] [TLP: RED] | In accordance  with designations accepted in TLP protocol  Default value [TLP: GREEN], unless otherwise specified |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 16 | Necessity of FinTsERT involvement | Necessity of FinTsERT involvement | CO | Where necessary | [Yes] | Necessity to engage FinTsERT to investigate the information security incident, the findings whereof shall be sent in the investigation notice |

APPENDIX 17. DATA PROVISION FORM NTF\_ORI\_INVESTIGATION -

FORM OF PROVISION BY INFORMATION EXCHANGE PARTICIPANTS OF DATA ABOUT THE FINDINGS OF INVESTIGATION OF AN OPERATIONAL RELIABILITY INCIDENT

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 1 | Type of notification | Type of notification | O | - | [NTF\_ORI\_  Investigation] | Pre-filled field |
| 2 | Relation to notification about identification of an operational reliability incident | Identifier of notification about identification of an operational reliability incident | O | - | In accordance  with AIPS FinTsERT format | Identifier of notification or response to the request previously sent  to FinTsERT by an information exchange  participant |
| 3 | Date and time | Date and time of actual occurrence of an operational reliability incident | O | - | In accordance with RFC 3339 | Moscow time [UTC +03:00] |
| 4 | Specification of data contained  in the notification about identification of an operational reliability incident | Code of type (area) of activity of financial institution | CO | Where necessary, to specify classification of operational reliability incident previously provided  in the notification about identification of an operational reliability incident | Selection of one value from the list:  From the classifier  "Classifier of information security and operational reliability incidents broken down by activities of credit  institutions, non-banking financial institutions and national payment system subjects and their constituent technological processes set forth  in [Appendix 11](#_bookmark31) | If a code of type (area) of activity of tier one and two financial institution is available, they shall be specified using ".", for instance: [Code 1].  [Code 2] |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 5 |  | Code of technological process |  |  | Selection of one value from the list:  From the classifier  "Classifier  of information security  and  operational reliability  incidents  broken down by  activities of credit  institutions,  non-banking financial  institutions  and national payment  system  subjects and their constituent  technological  processes"  set forth  in [Appendix 11](#_bookmark31)  The list depends  on the field "Code of type  (area) of activity  of financial  institution" | - |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
| 6 | Code of risk source | Selection of one value from the list:  From the classifier  "Risk sources"  set forth  in [Appendix 28](#_bookmark67) | - |
|  |  |
|  |  |
|  |  |
|  |  |
| 7 | Code of incident type | Selection of one value from the list:  From the classifier  "Classifier  of information security  and  operational reliability  incidents  broken down by  activities of credit  institutions,  non-banking financial  institutions  and national payment  system  subjects and their constituent  technological  processes"  set forth  in [Appendix 11](#_bookmark31)  The list depends  on the field "Code of technological  process' | - |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 8 |  | Code of incident |  |  | Selection of one value from the list:  From the classifier  "Classifier of information security and operational reliability incidents broken down by activities of credit  institutions, non-banking financial institutions and national payment system subjects and their constituent technological processes set forth  in [Appendix 11](#_bookmark31)  The list depends on the field "Code of type of information security incident" | - |
| 9 | "Information about information infrastructure facility  (the block is to be filled in separately for each information infrastructure facility having affected downtime or degradation of technological process) | Code of level of information infrastructure facility having affected downtime or degradation of technological process | CO | The block is to be filled in  in case of identification of information infrastructure facilities having affected  downtime or degradation of technological process and were not sent in the notification about identification of operational reliability incident | Selection of one value from the list:  From the classifier  "Types of objects and subjects" set forth  in [Appendix 28](#_bookmark67) | - |
| 10 | Code of type of information infrastructure facility having affected downtime or degradation of technological process | Selection of one value from the list:  From the classifier  "Types of objects and subjects" set forth  in [Appendix 28](#_bookmark67)  The list depends on the field "Code of level of object/subject" | - |
| 11 | Description of information infrastructure facility having affected downtime or degradation of technological process, in CPE format | In the format consistent with the recommendations of the Bank of Russia published on the official website | - |
| 12 | Information about an operational reliability incident | Date and time of resumption of services to the fullest extent | O | - | In accordance with RFC 3339 | Moscow time [UTC +03:00] |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 13 |  | Actual degradation share of the technological process affected by the operational reliability incident | O | - | Information about the value is specified in the form of decimal fraction accurate  to six decimal places (for instance, 0.000068) | Ratio between the total number of operations performed as part of technological process  during degradation of technological process, in terms of operational reliability incident  and expected number of operations performed  as part of technological process for the same period  in case of continuous  provision of services |
| 14 | Actual downtime and (or) degradation time of the technological process affected by the operational reliability incident | O | - | In minutes | The amount of time from occurrence of downtime  and (or) degradation time of the technological process related to provision of services until resumption of services to the fullest  extent is specified |
| 15 | Number of orders not performed as a result of incident occurrence | CO | In case of availability of information  in respect of the number of orders not performed as a result of incident occurrence | Integer number >0 | - |
| 16 | Amount of orders not performed as a result of incident occurrence | Amount accurate to two decimal places | - |
| 17 | Currency | From the All-Russian currency classifier | - |
| 18 | Adopted measures | O | - | Text field | Textual description of adopted measures for neutralisation  and avoidance of  repeated incident |
| 19 | Damage from the incident | Amount of direct losses | CO | If such losses are consequences of financial incident materialisation and where there is a possibility of their assessment | Amount in rubles  accurate to two decimal places | Direct losses of a financial organisation include losses reported in bookkeeping accounts of expenses and losses  and similar  accounts reflecting  receivables |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 20 |  | Amount of indirect losses | CO | If such losses are consequences of financial incident materialisation and where there is a possibility of their assessment | Amount in rubles  accurate to two decimal places | Indirect losses of a financial institution not reported in accounting but indirectly related to information security threat risk events including losses determined through calculation method in monetary terms |
| 21 | Qualitative losses | CO | Where an institution is subject to requirements on assessment of such losses under 716-P | In accordance  with the criteria of qualitative grading scale established in internal documents of the institution | Indirect losses of a financial institution not reported in accounting but indirectly related to information security threat risk events including losses determined based on expert opinion, where losses are not expressed in monetary terms through calculation method |
| 22 | Amount of potential losses | CO | If such losses are consequences of financial incident materialisation and where there is a possibility of their assessment | Amount in rubles  accurate to two decimal places | Indirect losses of a financial institution not reported in accounting but indirectly related to information security threat risk events including losses having not resulted in direct or indirect losses which could have arise upon realisation  of information security threat risk sources not identified by the financial institution and (or) upon unfavorable coincidence of circumstances |
| 23 | Measures taken by the credit institution for the purposes of receiving indemnity against incurred losses | CO | Where such measures were/are taken | Text field | - |
| 24 | Unique sequential identification number of an operational risk event | Unique sequential identification number of an operational risk event in the database of events corresponding to the given incident | CO | Only for credit institutions | Text field | - |

APPENDIX 18. LIST OF COMPUTER INCIDENTS AND COMPUTER ATTACKS

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of computer incident** | **Name of computer incident** | **Possible incident vectors** | **Notification criterion** | **Code of computer attack** | **Name of computer attack** | **Possible attack vectors** | **Notification criterion** |
| [DoS] | Slowed down operation of a resource as a result of "DoS (denial of service) attack" | [INT] - sent  to computer objects of the financial  institution | The fact of DoS-attack has been identified (active or completed)  with full or partial interruption of access or degradation of service used to perform banking and financial operations | [DoS] | "DoS (denial of service) attack" | [INT] - sent  to computer objects of the financial  institution | Attempts of DoS-attack (active or completed) have been identified in the reporting period, where the traffic usage profile exceeds the values established in internal regulations of the institution  (where no such value is available, is at least five times higher  than the standard value)  and the controlled resource continues to operate as expected without degradation of performance  There is information  about sources of malicious  activity |
| [Application compromise] | Successful use of vulnerability | [INT] - sent  to computer objects of the financial  institution | The fact of successful use of vulnerability of equipment or software of the institution has been recorded | [Exploit attempt] | Attempted use of vulnerability | [INT] - sent  to computer objects of the financial  institution | Attempted use of vulnerabilities of equipment and software of the institution has been identified in the reporting period.  There is information  about sources of malicious activity as well as description of used vulnerabilities  in the vulnerabilities description system or an expert opinion of the participant about a vulnerability not described in any vulnerabilities description system  was generated |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of computer incident** | **Name of computer incident** | **Possible incident vectors** | **Notification criterion** | **Code of computer attack** | **Name of computer attack** | **Possible attack vectors** | **Notification criterion** |
| [Malware infection] | Malware infection | [EXT] - oriented  on the client of financial  institution | The fact of execution of malicious code on the client's device enabling performance of financial operation without consent of the client.  There is an example of malicious code, its part or file suspicious in the opinion  of the participant previously transferred  to FinTsERT | [Infection attempt] | Attempted deployment of malware modules | [EXT] - oriented  on the client of financial  institution | Internet resources containing a malicious code or information enabling unauthorised access to information systems of information exchange participants and their clients used to provide (to receive) financial services, in particular, through unauthorised access to confidential information of clients were identified in the reporting period |
|  |  | [INT] - sent  to computer objects of the financial  institution | The fact of malicious code execution has been identified:   * on workstations, laptops, tablets of employees in charge of performance of functional duties; * on servers and network equipment of the institution; * on self-service machines, POS-terminal stations and ATM; * on other equipment of the institution which may be used to execute a malicious code or the compromise whereof   may in the participant's opinion cause damage to the institution |  |  | [INT] - sent  to computer objects of the financial  institution | A malicious code was identified in the reporting period:   * in the body of the e-mail message; * on workstations, laptops, tablets of employees in charge of performance of functional duties; * on servers and network equipment of the institution; * on self-service machines, POS-terminal stations and ATM; * on other equipment of the institution, on which a malicious code may be detected   the compromise whereof may in the participant's opinion cause damage to the institution. |
|  |  |  |  |  |  |  | There is an example of malicious code, its part or file suspicious  in the opinion of the participant not previously  sent to FinTsERT |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of computer incident** | **Name of computer incident** | **Possible incident vectors** | **Notification criterion** | **Code of computer attack** | **Name of computer attack** | **Possible attack vectors** | **Notification criterion** |
| [Account compromise] | Compromise of account | [EXT] - oriented  on the client of financial  institution | The fact of compromise of authentication data (logins, passwords) of the client enabling performance of financial operation without consent of the client has been identified.  There is information  about sources of compromise of account data or sources of malicious activity | [Login attempt] | Unsuccessful authorisation attempts | [EXT] - oriented  on the client of financial  institution | Facts of searching of authentication data (logins, passwords), e-mail addresses, server folders, URL of various web interfaces were identified or attempted receipt of any other data through the above method was recorded in the reporting period.  In the course of responding to the attack it was  established that searching was NOT a result of erroneous acts of a legitimate user, configuration errors or operation of vulnerability analysis tools used by the participant. |
|  |  |  |  |  |  |  | Number of unsuccessful searching attempts for each login exceeds the values established by internal regulations of the institution (in case such value is not available, exceeds 5 unsuccessful attempts). |
|  |  |  |  |  |  |  | There is information  about sources of malicious  activity |
|  |  | [INT] - sent  to computer objects of the financial  institution | The fact of compromise of authentication data (logins, passwords), e-mail addresses, server folders, URL of various web interfaces has been identified |  |  | [INT] - sent  to computer objects of the financial  institution |  |
| [Prohibited | Publication | [INT] - oriented | Information |  | | | |
| content] | on a controlled | on | prohibited |
|  | resource | computer | by the legislation |
|  | of information | facilities | of the Russian Federation was identified |
|  | prohibited | of the |  |
|  | by the legislation of the Russian | financial |  |
|  | Federation | institution |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of computer incident** | **Name of computer incident** | **Possible incident vectors** | **Notification criterion** | **Code of computer attack** | **Name of computer attack** | **Possible attack vectors** | **Notification criterion** |
| [Traffic | Capture of network | [INT] - oriented on  computer  objects of the  financial  institution | The fact of modification of  routing and address  information has been identified. The incident is relevant for those  financial institutions  containing  own AS, possessing  own blocks  of IP-addresses and announcing  them on borders of communications  service providers, renting IP-addresses  or have placed  their resources in rented  infrastructure  and BGP-hijack attacks  were in fact targeted  at the "lessor" |  | | | |
| hijacking] | traffic |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| [Unauthorised | unauthorised | [INT] - oriented  on  computer  facilities  of the  financial  institution | Identification of the fact of  unauthorised  modification of protected  information processed  in the controlled  resource or  transmitted through communications  channels |  | | | |
| modification] | modification |
|  | of |
|  | information |
|  |  |
|  |  |
|  |  |
| [Unauthorised  access] | unauthorised  disclosure  of  information | [INT] - oriented on  computer  objects of the  financial  institution | Identification of the fact of |  | | | |
| unauthorised |
| disclosure of protected |
| ("sensitive") |
| information (for instance, |
| github code, |
| where comments/logins |
| passwords were not deleted), |
| processed |
| in the controlled resource |
|  | or transmitted |
|  | through communications channels |
| [Attack using  resource] | Use of  controlled  resource  for  attacks | [INT] - oriented  on  computer  objects of the  financial  institution | The fact of use of |  | | | |
| controlled |
| resource for |
| attacking other information |
| infrastructure |
| facilities |
| [Without  attack] | Incident  not related  to computer  attack | [INT] - oriented  on  computer  objects of the  financial  institution | The fact of violation  or termination of operation  of CII facility  or power grid  used to arrange for interaction  of such facilities, not related to computer  attack of CII facility or  power grid |  | | | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of computer incident** | **Name of computer incident** | **Possible incident vectors** | **Notification criterion** | **Code of computer attack** | **Name of computer attack** | **Possible attack vectors** | **Notification criterion** |
| [Social engineering] | Social engineering | [EXT] - oriented  on the client of financial  institution | Successful attack targeted  at clients of the institution or counterparties which resulted in financial losses, leak of confidential information or other significant consequences with the use of:   * telephone call; * SMS-message; * e-mail; * instant messaging system (messengers); * other channel of communications with clients or counterparties.   Availability of information used  to apply social engineering methods, including telephone number,  e-mail address, technical letter header, text of the letter/SMS/ instant message etc. | [Social engineering] | Attempts of social engineering | [EXT] - oriented  on the client of financial  institution  [INT] - sent  to computer objects of the financial  institution | The facts of use of social engineering methods in respect of employees of the institution, clients of the institution or counterparties were identified in the reporting period, involving use of:   * telephone call; * SMS-message; * e-mail; * instant messaging system (messengers); * other information exchange channel within the institution or channel of interaction with clients or   counterparties.  Availability of information used  to apply social engineering methods, including telephone number,  e-mail address, technical letter header, text of the letter/SMS/ instant  message etc. |
|  |  |  |  |  |  |
|  |  | [INT] - oriented  to computer objects of the financial  institution | Successful attack targeted at employees of the institution which caused financial losses,  leak of confidential information or other significant consequences with the use of:   * telephone call; * SMS-message; * e-mail; * instant messaging system (messengers); * other information exchange channel within the   institution |  |  |  |  |
| [SIM] | Change  (replacement)  of mobile  subscriber's  identifier (IMSI),  mobile  equipment  identifier  (IMEI) or SIM-  card | [EXT] - oriented  on  the client of  financial  institution | Receiving an application  (notification, statement)  of the client on performance  of financial operation  without its consent using  a SIM-card  which was unlawfully  replaced |  | | | |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of computer incident** | **Name of computer incident** | **Possible incident vectors** | **Notification criterion** | **Code of computer attack** | **Name of computer attack** | **Possible attack vectors** | **Notification criterion** |
|  |  |  |  | [Phishing] | Identification of phishing mailout or resource | [EXT] - oriented  on the client of financial  institution | Internet resources containing information misinforming information exchange participants and their clients  as well as other persons cooperating with them due to  similarity of domain names, design and (or) content of the resource  to design and (or) content of official resources of the participant, its clients, other participants, their clients or counterparties were identified in the reporting period.  Availability of URL of the phishing resource.  Intermediate infrastructure elements of phishing infrastructure (intermediate servers for user proxying  to a phishing page) or registered but not announced domain names  with signs of phishing (though such domain name are de jure alleged  to have already been "published" in  Technical Internet Center registry etc.) have been additionally identified |
|  |  |  |
|  |  |  |
|  |  | [INT] - oriented  to computer objects of the financial  institution | Phishing messages containing in the e-mail address of the sender the words "bank", "cbr", "fincert",  "fsb", "fssp", "mvd", "pfrf",  "npf", "gosuslugi" in any spelling variant, as well as other words similar to the names pf public authorities, state automated systems, financial market  participants have been identified in the reporting period (according to technical headers they may not be sent from a legitimate mailing address).  Availability of sources of phishing mailout |
|  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Code of computer incident** | **Name of computer incident** | **Possible incident vectors** | **Notification criterion** | **Code of computer attack** | **Name of computer attack** | **Possible attack vectors** | **Notification criterion** |
|  |  |  |  | [Scanning] | Network scanning of controlled resource | [INT] - oriented  to computer objects of the financial  institution | Facts of scanning of controlled resources have been identified in the reporting period  and where the scanning traffic amount profile exceeds the values established by internal regulations of the institution (where no such value is available, it increased five-fold as compared to the standard value).  Availability of information about scanning sources |

APPENDIX 19. DATA PROVISION FORM NTF\_CI - FORM OF

PROVISION BY INFORMATION EXCHANGE PARTICIPANTS OF DATA ABOUT COMPUTER INCIDENTS

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 1 | Type of notification | Type of notification | O | - | [NTF\_CI] | Pre-filled field |
| 2 | Description of computer incident | Description of computer incident | N | - | Text field | Textual description of computer incident (including additional information on the method of CI realisation, method of CI identification etc.). Where a computer incident is identified  using information from the bulletin of the Bank of Russia or NCCCI, the number of such bulletin is to be specified |
| 3 | Classification of computer incident | Vector | O | - | [EXT]  [INT] | In accordance with the classifier of computer incidents set forth in [Appendix 18](#_bookmark38) |
| 4 | Type of computer incident | O | - | [DoS]  [Application compromise] [Malware infection] [Account compromise] [Prohibited content] [Social engineering] [Traffic hijacking] [Unauthorised modification] [Unauthorised access] [SIM]  [Attack using resource] [Without attack] | In accordance with the classifier of computer incidents set forth in [Appendix 18](#_bookmark38) |
| 5 | Date and time of detection | Date and time of computer incident identification | O | - | In accordance with RFC 3339 | Moscow time [UTC +03:00] |
| 6 | Information about facilities being the target of computer incident | Dataset | CO | The structure of data depends on the field "Type of computer incident" and is specified in the tab  "Information about  CI facilities" | - |
| 7 | Information about malicious activity objects having caused the computer incident | Dataset | CO | The structure of data depends on the field "Type of computer incident" and is specified in the tab  "Information about  MA objects" | - |
| 8 | Information about unlawful disclosure of PD | Supposed reasons having caused violation of PD subjects' rights | CO | The block is to be filled in  in case, when the computer incident results in PD leak | Text field | Description of events having caused unlawful disclosure of information. The filed is to be filled in, where the field  "Description of computer incident" has insufficient information about unlawful  disclosure of PD |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 9 |  | Characteristics of PD |  |  | Text field | Information characterising unlawfully disclosed PD shall be specified, including the type of the subject whose PD were disclosed, the structure of unlawfully disclosed PD, the number and relevance of entries etc. |
| 10 | Supposed damage caused to the PD subjects' rights | Text field | Description of supposed damage which may be caused to the subjects upon use of unlawfully disclosed information |
| 11 | Full name of the person authorised by the operator to interact  with Roskomnadzor  on the incident | Text field | - |
| 12 | Mobile telephone of the person authorised to interact  with Roskomnadzor  on the incident | In accordance with the Russian numbering system and plan | - |
| 13 | E-mail address for sending information about notification | In the format  of e-mail address | - |
| 14 | Assessment of consequences of computer incident | Impact on confidentiality | CO | In case the specified consequences have occurred | [High] [Low] | - |
| 15 | Impact on integrity | [High] [Low] | - |
| 16 | Impact on availability | [High] [Low] | - |
| 17 | Measures taken to respond  to computer  incident | Description of acts taken in the process of responding to the computer incident | N | - | Text field | - |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 18 | Relation to other notifications | Type of related notification | CO | To be filled in where the Bank of Russia was previously sent a notification related  to the current notification | [NTF\_OWC] [NTF\_ISI] [NTF\_ORI] [NTF\_CI] [NTF\_CA] [NTF\_VLN] | [NTF\_OWC] - notification   * about identified cases and (or) attempts of funds transfers without consent of the client as well as identified cases   and (or) attempts of carrying out operations aimed at consummation of financial transactions using financial platform, not relying on the financial platform participant's will, [NTF\_ISI] - notification about identification of an information security incident or the findings of investigation of an information security incident [NTF\_ORI] - notification   * about identification of an operational reliability incident or * the findings of investigation of an operational reliability incident   [NTF\_CI] - notification   * about computer incidents [NTF\_CA] - notification * about computer attacks [NTF\_VLN] - notification * about identified vulnerabilities |
| 19 | Type of relation to other notifications | [Preceding event]  [Subsidiary event] [Related event] [Specification of information  about event] | - |
| 20 | Registration number of notification | In accordance with AIPS FinTsERT format | Identifier of notification or response to the request previously sent to FinTsERT by an information exchange participant |
| 21 | Restrictive TLP marker | Restrictive marker for distribution of information from the given notification | N | - | [TLP: WHITE] [TLP: GREEN] [TLP: AMBER] [TLP: RED] | In accordance with designations accepted in TLP protocol.  Default value [TLP: GREEN], unless otherwise specified |
| 22 | Necessity of FinTsERT involvement | Necessity of FinTsERT involvement to rectify the consequences of the computer incident | CO | Where necessary | [Yes] | - |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Code of computer incident** | **Name of computer incident** | **Technical information about facilities being the target of computer incident** | | | | |
| **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| [DoS] | Slowed down | Name of controlled  resource | O | - | Text field | - |
|  | operation of a resource |  |  |  |
|  | as a result of |  |  |  |
|  | "DoS (denial of service) |  |  |  |
|  | attack" |  |  |  |
|  |  | Category of controlled resource | CO | If it is a CII object | [No relevance category]  [Third relevance  category]  [Second relevance  category]  [First relevance  category] | - |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  | Code of level of object/subject | O | - | From the classifier  "Types of objects and subjects"  set forth  in [Appendix 28](#_bookmark67) | - |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  | Code of type of object/subject | O | - | The list depends on the field "Code of level  of attacked object/  subject".  From the classifier  "Types of objects and subjects"  set forth  in [Appendix 28](#_bookmark67) | - |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  | Availability of Internet connection | O | - | [Yes] | Pre-filled field |
|  |  | Country/region | O | - | In ISP-3166-2 format | - |
|  |  | IPv4-address of controlled resource | CO | One of the fields must be filled in | List of IP-addresses | - |
|  |  | IPv6-address of controlled |  |  |  |
|  |  | resource |  |  |  |
|  |  | Domain name of controlled resource |  | List of domain names |  |
|  |  | URI-address of controlled resource |  | List of URI-addresses |  |
|  |  | Attacked network | CO | In case of availability of | Text field | - |
|  |  | service and port/ |  | the relevant |  |  |
|  |  | protocol |  | information |  |  |
| [Application compromise] | Successful use of vulnerability | Name of controlled resource | O | - | Text field | - |
| Category of controlled resource | CO | If it is a CII object | [No relevance category]  [Third relevance category] [Second relevance category] [First relevance  category] | - |
| Code of level of object/subject | O | - | From the classifier  "Types of objects and subjects" set forth  in [Appendix 28](#_bookmark67) | - |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Code of computer incident** | **Name of computer incident** | **Technical information about facilities being the target of computer incident** | | | | |
| **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
|  |  | Code of type of object/subject | O | - | The list depends on the field "Code of level of attacked object/subject".  From the classifier  "Types of objects and subjects" set forth  in [Appendix 28](#_bookmark67) | - |
| Availability of Internet connection | O | - | [Yes]/[No] | - |
| Country/region | O | - | In ISP-3166-2 format | - |
| IPv4-address of controlled resource | CO | One of the fields must be filled in | List of IP-addresses | - |
| IPv6-address of controlled resource |
| Domain name of controlled resource | List of domain names |
| URI-address of controlled resource | List of URI-addresses |
| Attacked network service and port/protocol | CO | In case of availability of respective information | Text field | - |
| [Malware infection] | Malware infection | Name of controlled resource | O | - | Text field | - |
| Category of controlled resource | CO | If it is a CII object | [No relevance category]  [Third relevance category] [Second relevance category] [First relevance  category] | - |
| Code of level of object/subject | O | - | From the classifier  "Types of objects and subjects" set forth  in [Appendix 28](#_bookmark67) | - |
| Code of type of object/subject | O | - | The list depends on the field "Code of level of attacked object/subject".  From the classifier  "Types of objects and subjects" set forth  in [Appendix 28](#_bookmark67) | - |
| Availability of Internet connection | O | - | [Yes]/[No] | - |
| Country/region | O | - | In ISP-3166-2 format | - |
| IPv4-address of controlled resource | CO | One of the fields must be filled in | List of IP-addresses | - |
| IPv6-address of controlled resource |
| Domain name of controlled resource | List of domain names |
| URI-address of controlled resource | List of URI-addresses |
| e-mail address of controlled object | List of e-mail addresses |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Code of computer incident** | **Name of computer incident** | **Technical information about facilities being the target of computer incident** | | | | |
| **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
|  |  | Attacked network service and port/protocol | CO | In case of availability of respective information | Text field | - |
| [Account compromise] | Compromise of account | Name of controlled resource | O | - | Text field | - |
| Category of controlled resource | CO | If it is a CII object | [No relevance category]  [Third relevance category] [Second relevance category] [First relevance  category] | - |
| Code of level of object/subject | O | - | From the classifier  "Types of objects and subjects" set forth  in [Appendix 28](#_bookmark67) | - |
| Code of type of object/subject | O | - | The list depends on the field "Code of level of attacked object/subject".  From the classifier  "Types of objects and subjects" set forth  in [Appendix 28](#_bookmark67) | - |
| Availability of Internet connection | O | - | [Yes]/[No] | - |
| Country/region | O | - | In ISP-3166-2 format | - |
| IPv4-address of controlled resource | CO | One of the fields must be filled in | List of IP-addresses | - |
| IPv6-address of controlled resource |
| Domain name of controlled resource | List of domain names |
| URI-address of controlled resource | List of URI-addresses |
| e-mail address of controlled object | List of e-mail addresses |
| Attacked network service and port/protocol | CO | In case of availability of respective information | Text field | - |
| [Prohibited content] | Publication  on the controlled resource of information prohibited by the legislation of the Russian Federation | Name of controlled resource | O | - | Text field | - |
| Category of controlled resource | CO | If it is a CII object | [No relevance category]  [Third relevance category] [Second relevance category] [First relevance  category] | - |
| Code of level of object/subject | O | - | From the classifier  "Types of objects and subjects" set forth  in [Appendix 28](#_bookmark67) | - |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Code of computer incident** | **Name of computer incident** | **Technical information about facilities being the target of computer incident** | | | | |
| **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
|  |  | Code of type of object/subject | O | - | The list depends on the field "Code of level of attacked object/subject".  From the classifier  "Types of objects and subjects" set forth  in [Appendix 28](#_bookmark67) | - |
| Availability of Internet connection | O | - | [Yes]/[No] | - |
| Country/region | O | - | In ISP-3166-2 format | - |
| IPv4-address of controlled resource | CO | One of the fields must be filled in | List of IP-addresses | - |
| IPv6-address of controlled resource |
| Domain name of controlled resource | List of domain names |
| URI-address of controlled resource | List of URI-addresses |
| [Traffic hijacking] | Capture of network traffic | Name of controlled resource | O | - | Text field | - |
| Category of controlled resource | CO | If it is a CII object | [No relevance category]  [Third relevance category] [Second relevance category] [First relevance  category] | - |
| Code of level of object/subject | O | - | From the classifier  "Types of objects and subjects" set forth  in [Appendix 28](#_bookmark67) | - |
| Code of type of object/subject | O | - | The list depends on the field "Code of level of attacked object/subject".  From the classifier  "Types of objects and subjects" set forth  in [Appendix 28](#_bookmark67) | - |
| Availability of Internet connection | O | - | [Yes]/[No] | - |
| Country/region | O | - | In ISP-3166-2 format | - |
| AS-Path to the controlled autonomous system (ASN) | O | - | Text field | - |
| [Unauthorised modification] | Unauthorised modification of information | Name of controlled resource | O | - | Text field | - |
| Category of controlled resource | CO | If it is a CII object | [No relevance category]  [Third relevance category] [Second relevance category] [First relevance  category] | - |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Code of computer incident** | **Name of computer incident** | **Technical information about facilities being the target of computer incident** | | | | |
| **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
|  |  | Code of level of object/subject | O | - | From the classifier  "Types of objects and subjects" set forth  in [Appendix 28](#_bookmark67) | - |
| Code of type of object/subject | O | - | The list depends on the field "Code of level of attacked object/subject".  From the classifier  "Types of objects and subjects" set forth  in [Appendix 28](#_bookmark67) | - |
| Availability of Internet connection | O | - | [Yes]/[No] | - |
| Country/region | O | - | In ISP-3166-2 format | - |
| IPv4-address of controlled resource | CO | One of the fields must be  filled in | List of IP-addresses | - |
| IPv6-address of controlled resource |
| Domain name of controlled resource | List of domain names |
| URI-address of controlled resource | List of URI-addresses |
| Attacked network service and port/protocol | CO | In case of availability of respective information | Text field | - |
| [Unauthorised access] | Unauthorised disclosure of information | Name of controlled resource | O | - | Text field | - |
| Category of controlled resource | CO | If it is a CII object | [No relevance category]  [Third relevance category] [Second relevance category] [First relevance  category] | - |
| Code of level of object/subject | O | - | From the classifier  "Types of objects and subjects" set forth  in [Appendix 28](#_bookmark67) | - |
| Code of type of object/subject | O | - | The list depends on the field "Code of level of attacked object/subject".  From the classifier  "Types of objects and subjects" set forth  in [Appendix 28](#_bookmark67) | - |
| Availability of Internet connection | O | - | [Yes]/[No] | - |
| Country/region | O | - | In ISP-3166-2 format | - |
| IPv4-address of controlled resource | CO | One of the fields must be filled in | List of IP-addresses | - |
| IPv6-address of controlled resource |
| Domain name of controlled resource | List of domain names |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Code of computer incident** | **Name of computer incident** | **Technical information about facilities being the target of computer incident** | | | | |
| **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
|  |  | URI-address of controlled resource |  |  | List of URI-addresses |  |
| e-mail address of controlled object | List of e-mail addresses |
| Attacked network service and port/protocol | CO | In case of availability of respective information | Text field | - |
| [Social engineering] | Social engineering | Code of level of object/subject | O | - | [Subject] | Pre-filled field |
| Code of type of object/subject | O | - | [Employee] [Client] [Partner] | From the classifier "Type of attacked object-subject" |
| [SIM] | Change (spoofing) of a mobile subscriber identifier (IMSI), mobile equipment identifier (IMEI) or a SIM-card | - | | | | |
| [Attack using resource] | Use of controlled resource for attacks | Name of controlled resource | O | - | Text field | - |
| Category of controlled resource | CO | If it is a CII object | [No relevance category]  [Third relevance category] [Second relevance category] [First relevance  category] | - |
| Code of level of object/subject | O | - | From the classifier  "Types of objects and subjects" set forth  in [Appendix 28](#_bookmark67) | - |
| Code of type of object/subject | O | - | The list depends on the field "Code of level of attacked object/subject".  From the classifier  "Types of objects and subjects" set forth  in [Appendix 28](#_bookmark67) | - |
| Availability of Internet connection | O | - | [Yes] | Pre-filled field |
| Country/region | O | - | In ISP-3166-2 format | - |
| IPv4-address of controlled resource | CO | One of the fields must be filled in | List of IP-addresses | - |
| IPv6-address of controlled resource |
| Domain name of controlled resource | List of domain names |
| URI-address of controlled resource | List of URI-addresses |
| e-mail address of controlled object | List of e-mail addresses |
| Attacked network service and port/protocol | CO | In case of availability of respective information | Text field | - |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Code of computer incident** | **Name of computer incident** | **Technical information about facilities being the target of computer incident** | | | | |
| **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| [Without attack] | Incident  not related  to computer attack | Name of controlled resource | O | - | Text field | - |
| Category of controlled resource | CO | If it is a CII object | [No relevance category]  [Third relevance category] [Second relevance category] [First relevance  category] | - |
| Code of level of object/subject | O | - | From the classifier  "Types of objects and subjects" set forth  in [Appendix 28](#_bookmark67) | - |
| Code of type of object/subject | O | - | The list depends on the field "Code of level of attacked object/subject".  From the classifier  "Types of objects and subjects" set forth  in [Appendix 28](#_bookmark67) | - |
| Availability of Internet connection | O | - | [Yes]/[No] | - |
| Country/region | O | - | In ISP-3166-2 format | - |
| IPv4-address of controlled resource | CO | One of the fields must be filled in | List of IP-addresses | - |
| IPv6-address of controlled resource |
| Domain name of controlled resource | List of domain names |
| URI-address of controlled resource | List of URI-addresses |
| e-mail address of controlled object | List of e-mail addresses |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Code of computer incident** | **Name of computer incident** | **Information about malicious activity objects or subjects having caused the computer incident** | | | | |
| **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| [DoS] | Slowed down operation of a resource as a result of  "DoS (denial of service) attack" | Type of attack | O | - | [DoS – Flood] [DoS – Vuln] [DDos] | - |
| OSI level | O | - | [L2/3]  [L3]  [L4]  [L6]  [L7] | [L2/3] - channel/network level  [L3] - network level  [L4] - transport level [L6] - data representation level  [L7] - application level |
| IPv4-address of malicious object | CO | IPv4-address of malicious object has been identified | List of IP-addresses or csv-file | At least one field is to be filled in |
| IPv6-address of a malicious object | IPv6-address of a malicious object has been identified |
| Domain name of malicious object | CO | Domain name of malicious object has been identified | List of domain names or csv-file |
| Country of malicious object location | N | - | List of three-letter codes of countries in accordance with ISO 3166 | - |
| PPS (packets per second) | CO | At least one field is to be filled in | Real number | - |
| Mbit/s (megabits per second) | Real number | - |
| RPS (requests per second) | Real number | - |
| FPS (frames per second) | Real number | - |
| List of used vulnerabilities | CO | Fact of use of vulnerabilities has been identified | - | List of used vulnerabilities of software or hardware in the selected system of description of security vulnerabilities (for instance, CVE, TDB FSTEC) |
| Name of system of description of security vulnerabilities | Text field |
| [Application compromise] | Successful use of vulnerability | IPv4-address of malicious object | CO | IPv4-address of malicious object has been identified | List of IP-addresses | - |
| IPv6-address of a malicious object | IPv6-address of a malicious object has been identified | - |
| Domain name of malicious object | Domain name of malicious object has been identified | List of domain names | - |
| URI-address of malicious object | URI-address of malicious object has been identified | List of URI-addresses | - |
| e-mail-address of malicious object or subject | E-mail-address of malicious object or subject has been identified | List of e-mail-addresses | - |
| Vulnerability | CO | In case the identified vulnerability is described in any system of description of vulnerabilities | List of used vulnerabilities of security of software or hardware, from the respective catalogue (for instance, CVE, TDB FSTEC etc.) | One of blocks must be filled in |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Code of computer incident** | **Name of computer incident** | **Information about malicious activity objects or subjects having caused the computer incident** | | | | |
| **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
|  |  | Name of system of description of vulnerabilities |  |  | Text field |  |
| Description of vulnerability | CO | In case the identified vulnerability is not described in any system of description of vulnerabilities | Text field |
| Description of computer object, in which vulnerability was used | O | - | In the format consistent with the recommendations of the Bank of Russia published on the official website | - |
| [Malware infection] | Malware infection | IPv4-address of malicious object | CO | IPv4-address of malicious object has been identified | List of IP-addresses | - |
| IPv6-address of a malicious object | IPv6-address of a malicious object has been identified | - |
| Domain name of malicious object | Domain name of malicious object has been identified | List of domain names | - |
| URI-address of malicious object | URI-address of malicious object has been identified | List of URI-addresses | - |
| e-mail-address of malicious object or subject | E-mail-address of malicious object or subject has been identified | List of e-mail-addresses | - |
| Name of antivirus having identified malware infection | CO | If the malware was identified by antivirus | Text field | - |
| Description and classification of malicious software | N | - | Text field | - |
| Network activity | CO | Where information about network activity of malware is available | Text field | - |
| Vulnerability | CO | Where the fact of use of vulnerabilities by malware has been identified | List of used vulnerabilities of security of software or hardware, from the respective catalogue (for instance, CVE, TDB FSTEC etc.) | - |
| Name of system of description of vulnerabilities | Text field | - |
| Description of vulnerability not described in any system of description of vulnerabilities | Text field | - |
| Malware file | CO | One of the fields must be filled in | File | - |
| URL for downloading | Text field | - |
| Hash sum | O | - | Text field | - |
| Hashing algorithm |  | - | [SHA256] [SHA1]  [MD5] | - |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Code of computer incident** | **Name of computer incident** | **Information about malicious activity objects or subjects having caused the computer incident** | | | | |
| **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| [Account compromise] | Compromise of account | IPv4-address of malicious object | CO | IPv4-address of malicious object has been identified | List of IP-addresses | - |
| IPv6-address of a malicious object | IPv6-address of a malicious object has been identified | - |
| Domain name of malicious object | Domain name of malicious object has been identified | List of domain names | - |
| Login of compromised account | O | - | Text field | - |
| Privileges of compromised account | O | - | Text field | - |
| Compromise method | CO | In case of availability of respective information | Text field | - |
| [Prohibited content] | Publication on the controlled resource of information prohibited by the legislation of the Russian Federation | IPv4-address of malicious object | CO | IPv4-address of malicious object has been identified | List of IP-addresses | - |
| IPv6-address of a malicious object | IPv6-address of a malicious object has been identified | - |
| Domain name of malicious object | Domain name of malicious object has been identified | List of domain names | - |
| URI-address of malicious object | URI-address of malicious object has been identified | List of URI-addresses | - |
| [Traffic hijacking] | Capture of network traffic | Number of dummy autonomous system (ASN) | O | - | Text field | - |
| AS name | O | - | Text field | - |
| LIR name | O | - | Text field | - |
| Reference to Looking Glass | CO | In case of availability of | Text field | - |
| Authentic prefix | N | - | Text field | - |
| Dummy prefix | N | - | Text field | - |
| [Unauthorised modification] | Unauthorised modification of information | IPv4-address of malicious object | CO | IPv4-address of malicious object has been identified | List of IP-addresses | - |
| IPv6-address of a malicious object | IPv6-address of a malicious object has been identified | - |
| Domain name of malicious object | Domain name of malicious object has been identified | List of domain names | - |
| URI-address of malicious object | URI-address of malicious object has been identified | List of URI-addresses | - |
| [Unauthorised access] | Unauthorised disclosure of information | IPv4-address of malicious system | CO | IPv4-address of malicious system or object has been identified | List of IP-addresses | - |
| IPv6-address of malicious system | IPv6-address of malicious system or object has been identified | - |
| Domain name of malicious system | Domain name of malicious system of object has been identified | List of domain names | - |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Code of computer incident** | **Name of computer incident** | **Information about malicious activity objects or subjects having caused the computer incident** | | | | |
| **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
|  |  | e-mail-address of malicious object |  | E-mail-address of malicious system or object has been identified | List of e-mail-addresses | - |
| [Social engineering] | Social engineering | IPv4-address of malicious object | CO | IPv4-address of malicious object has been identified | List of IP-addresses | - |
| IPv6-address of a malicious object | IPv6-address of a malicious object has been identified | - |
| Domain name of malicious object | Domain name of malicious object has been identified | List of domain names | - |
| URI-address of malicious object | URI-address of malicious object has been identified | List of URI-addresses | - |
| e-mail-address of malicious object or subject | E-mail-address of malicious object or subject has been identified | List of e-mail-addresses | - |
| Mobile telephone communications subscriber's number of malicious subject | Mobile telephone number of malicious subject has been identified | List of mobile telephone numbers in accordance with the Russian numbering system and plan | - |
| Interaction channel | O | - | [Telephone call] [SMS]  [E-mail] [Instant messaging system]  [Website]  [Other channel] | - |
| Message text | CO | "Interaction channel" = { [SMS], [E-mail], [Instant messaging system]} | Text field or txt-file | - |
| [SIM] | Change (spoofing) of a mobile subscriber identifier (IMSI), mobile equipment identifier (IMEI) or a SIM-card | Mobile telephone communications subscriber's number | O | - | In accordance with the Russian numbering system and plan | - |
| IMSI | O | - | Text field | - |
| Communications provider | N | - | Text field | - |
| Date of IMSI change | N | - | In accordance with RFC 3339 | Moscow time [UTC +03:00] |
| [Attack using resource] | Use of controlled resource for attacks | IPv4-address of malicious object | CO | IPv4-address of malicious object has been identified | List of IP-addresses | - |
| IPv6-address of a malicious object | IPv6-address of a malicious object has been identified | - |
| Domain name of malicious object | Domain name of malicious object has been identified | List of domain names | - |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Code of computer incident** | **Name of computer incident** | **Information about malicious activity objects or subjects having caused the computer incident** | | | | |
| **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
|  |  | URI-address of malicious object |  | URI-address of malicious object has been identified | List of URI-addresses | - |
| e-mail-address of malicious object or subject | E-mail-address of malicious object or subject has been identified | List of e-mail-addresses | - |
| Vulnerability | CO | Where the identified vulnerability is described  in any system of description of vulnerabilities | List of used vulnerabilities of security of software or hardware, from the respective catalogue (for instance, CVE, TDB FSTEC etc.) | One of blocks must be filled in |
| Name of system of description of vulnerabilities | Text field |
| Description of vulnerability | CO | In case the identified vulnerability is not described in any system of description of vulnerabilities | Text field |
| Description of computer object, in which vulnerability was used | O | - | In the format consistent with the recommendations of the Bank of Russia published on the official website | - |
| Malware file | CO | One of the fields must be  filled in | File | - |
| URL for downloading | Text field | - |
| Hash sum | O | - | Text field | - |
| Hashing algorithm | - | [SHA256] [SHA1]  [MD5] | - |
| [Without attack] | Incident  not related  to computer  attack | - | | | | |

APPENDIX 20. DATA PROVISION FORMS NTF\_CI, PRE-FILLED FOR COMPUTER INCIDENTS

|  |  |
| --- | --- |
| **Code of computer incident** | **Name of computer incident** |
| [[DoS](#_bookmark41)] | Slowed down operation of a resource as a result of "DoS (denial of service) attack" |
| [[Application compromise](#_bookmark42)] | Successful use of vulnerability |
| [[Malware infection](#_bookmark43)] | Malware infection |
| [[Account compromise](#_bookmark44)] | Compromise of account |
| [[Prohibited content](#_bookmark45)] | Publication on the controlled resource of information prohibited by the legislation of the Russian Federation |
| [[Social engineering](#_bookmark46)] | Social engineering |
| [[Traffic hijacking](#_bookmark47)] | Capture of network traffic |
| [[Unauthorised modification](#_bookmark48)] | Unauthorised modification of information |
| [[Unauthorised access](#_bookmark49)] | Unauthorised disclosure of information |
| [[SIM](#_bookmark50)] | Change (spoofing) of a mobile subscriber identifier (IMSI), mobile equipment identifier (IMEI) or a SIM-card |
| [[Attack using resource](#_bookmark51)] | Use of controlled resource for attacks |
| [[Without attack](#_bookmark52)] | Incident not related to computer attack |

### Data provision form NTF\_CI\_DoS - Form of provision of data about a computer incident related to slowed down operation of a resource as a result of "DoS (denial of service) attack"

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 1 | Type of notification | Type of notification | O | - | [NTF\_CI\_DoS] | Pre-filled field |
| 2 | Description of computer incident | Description of computer incident | N | - | Text field | Textual description of computer incident (including additional information on the method of CI realisation, method of CI identification etc.). Where a computer incident is identified  using information from the bulletin of the Bank of Russia or NCCCI, the number of such bulletin is to be specified |
| 3 | Classification of computer incident | Vector | O | - | [INT] | Pre-filled field |
| 4 | Type of computer incident | O | - | [DoS] | Pre-filled field |
| 5 | Date and time of detection | Date and time of computer incident identification | O | - | In accordance with RFC 3339 | Moscow time [UTC +03:00] |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 6 | Information about facilities being the target of computer incident | Name of controlled information resource | O | - | Text field | - |
| 7 |  | Category of controlled resource | CO | If it is a CII object | [No relevance category]  [Third relevance category] [Second relevance category] [First relevance  category] | - |
| 8 |  | Code of level of attacked object/subject | O | - | From the classifier  "Types of objects and subjects" set forth  in [Appendix 28](#_bookmark67) | - |
| 9 |  | Code of type of attacked object/subject | O | - | The list depends on the field "Code of level of attacked object/subject". | The list depends on the field  "Code of level of attacked object/subject" |
|  |  |  |  |  | From the classifier  "Types of objects and subjects" set forth  in [Appendix 28](#_bookmark67) |  |
| 10 |  | Availability of Internet connection | O | - | [Yes] | Pre-filled field |
| 11 |  | Country/region | O | - | In ISP-3166-2 format | - |
| 12 |  | IPv6-address of attacked resource | CO | One of the fields must be filled in | List of IP-addresses | - |
| 13 |  | IPv6-address of attacked resource |  |  |  |  |
| 14 |  | Domain name of attacked resource |  |  | List of domain names |  |
| 15 |  | URI-address of attacked resource |  |  | List of URI-addresses |  |
| 16 |  | Attacked network service and port/protocol | CO | In case of availability of respective information | Text field | - |
| 17 | Information about malicious activity objects having caused the computer incident | Type of attack | O | - | [DoS – Flood] [DoSVuln] [DDos] | - |
| 18 | OSI level | O | - | [L2/3]  [L3]  [L4]  [L6]  [L7] | [L2/3] - channel/network level  [L3] - network level  [L4] - transport level [L6] - data representation level  [L7] - application level |
| 19 | IPv4-address of malicious object | CO | IPv4-address of malicious object has been identified | List of IP-addresses or csv-file | At least one field is to be filled in |
| 20 | IPv6-address of a malicious object | IPv6-address of a malicious object has been identified |
| 21 | Domain name of malicious object | CO | Domain name of malicious object has been identified | List of domain names or csv-file |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 22 |  | Country of malicious object location | N | - | List of three-letter codes of countries in accordance with ISO 3166 | - |
| 23 | PPS (packets per second) | CO | At least  one field is to be filled in | Real number | - |
| 24 | Mbit/s (megabits per second) | Real number | - |
| 25 | RPS (requests per second) | Real number | - |
| 26 | FPS (frames per second) | Real number | - |
| 27 | List of used vulnerabilities | CO | Fact of use of vulnerabilities has been identified | - | List of used vulnerabilities of software or hardware in the selected system of description of security vulnerabilities (for instance, CVE, TDB FSTEC) |
| 28 | Name of system of description of security vulnerabilities | Text field |
| 29 | Assessment of consequences of computer incident | Impact on confidentiality | CO | In case the specified consequences have occurred | [High] [Low] | - |
| 30 | Impact on integrity | [High] [Low] | - |
| 31 | Impact on availability | [High] [Low] | - |
| 32 | Measures taken to respond  to computer  incident | Description of acts taken in the process of responding to the computer incident | N | - | Text field | - |
| 33 | Relation to other notifications | Type of related notification | CO | To be filled in where the Bank of Russia was previously sent a notification related  to the current notification | [NTF\_OWC] [NTF\_ISI] [NTF\_ORI] [NTF\_CI] [NTF\_CA] [NTF\_VLN] | [NTF\_OWC] - notification   * about identified cases and (or) attempts of funds transfers without consent of the client as well as identified cases   and (or) attempts of carrying out operations aimed at consummation of financial transactions using financial platform, not relying on the financial platform participant's will, [NTF\_ISI] - notification about identification of an information security incident or the findings of investigation of an information security incident [NTF\_ORI] - notification   * about identification of an operational reliability incident or * the findings of investigation of an operational reliability incident   [NTF\_CI] - notification   * about computer incidents [NTF\_CA] - notification * about computer attacks [NTF\_VLN] - notification * about identified vulnerabilities |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 34 |  | Type of relation to other notifications |  |  | [Preceding event]  [Subsidiary event] [Related event] [Specification of information  about event] | - |
| 35 | Registration number of notification | In accordance with AIPS FinTsERT format | Identifier of notification or response to the request previously sent to FinTsERT by an information exchange participant |
| 36 | Restrictive TLP marker | Restrictive marker for distribution of information from the given notification | N | - | [TLP: WHITE] [TLP: GREEN] [TLP: AMBER] [TLP: RED] | In accordance with designations accepted in TLP protocol.  Default value [TLP: GREEN], unless otherwise specified |
| 37 | Necessity of FinTsERT involvement | Necessity of FinTsERT involvement to rectify the consequences of the computer incident | CO | Where necessary | [Yes] | - |

**Data provision form NTF\_CI\_Application compromise - Form of provision of data about a computer incident related to successful use of vulnerability**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 1 | Type of notification | Type of notification | O | - | [NTF\_CI\_Application compromise] | Pre-filled field |
| 2 | Description of computer incident | Description of computer incident | N | - | Text field | Textual description of computer incident (including additional information on the method of CI realisation, method of CI identification etc.). Where a computer incident is identified  using information from the bulletin of the Bank of Russia or NCCCI, the number of such bulletin is to be specified |
| 3 | Classification of computer incident | Vector | O | - | [INT] | Pre-filled field |
| 4 |  | Type of computer incident | O | - | [Application compromise] | Pre-filled field |
| 5 | Date and time of detection | Date and time of computer incident identification | O | - | In accordance with RFC 3339 | Moscow time [UTC +03:00] |
| 6 | Information about facilities being the target of computer incident | Name of controlled information resource | O | - | Text field | - |
| 7 | Category of controlled resource | CO | If it is a CII object | [No relevance category]  [Third relevance category] [Second relevance category] [First relevance  category] | - |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 8 |  | Code of level of attacked object/subject | O | - | From the classifier  "Types of objects and subjects" set forth  in [Appendix 28](#_bookmark67) | - |
| 9 | Code of type of attacked object/subject | O | - | The list depends on the field "Code of level of attacked object/subject". | The list depends on the field  "Code of level of attacked object/subject" |
|  |  |  |  | From the classifier  "Types of objects and subjects" set forth  in [Appendix 28](#_bookmark67) |  |
| 10 | Availability of Internet connection | O | - | [Yes]/[No] | - |
| 11 | Country/region | O | - | In ISP-3166-2 format | - |
| 12 | IPv6-address of attacked resource | CO | One of the fields must be filled in | List of IP-addresses | - |
| 13 | IPv6-address of attacked resource |  |  |  |  |
| 14 | Domain name of attacked resource |  |  | List of domain names |  |
| 15 | URI-address of attacked resource |  |  | List of URI-addresses |  |
| 16 | Attacked network service and port/protocol | CO | In case of availability of respective information | Text field | - |
| 17 | Information about malicious activity objects having caused the computer incident | IPv4-address of malicious object | CO | IPv4-address of malicious object has been identified | List of IP-addresses | - |
| 18 | IPv6-address of a malicious object | IPv6-address of a malicious object has been identified | - |
| 19 | Domain name of malicious object | Domain name of malicious object has been identified | List of domain names | - |
| 20 | URI-address of malicious object | URI-address of malicious object has been identified | List of URI-addresses | - |
| 21 | e-mail-address of malicious object or subject | E-mail-address of malicious object or subject has been identified | List of e-mail addresses | - |
| 22 | Vulnerability | CO | In case the identified vulnerability is described in any system of description of vulnerabilities | List of used vulnerabilities of security of software or hardware, from the respective catalogue (for instance, CVE, TDB FSTEC etc.) | One of blocks must be filled in |
| 23 | Name of system of description of vulnerabilities | Text field |
| 24 | Description of vulnerability | CO | In case the identified vulnerability is not described in any system of description of vulnerabilities | Text field |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 25 |  | Description of computer object, in which vulnerability was used | O | - | In the format consistent with the recommendations of the Bank of Russia published on the official website | - |
| 26 | Information about unlawful disclosure of PD | Supposed reasons having caused violation of PD subjects' rights | CO | The block is to be filled in  in case, when the computer incident results in PD leak | Text field | Description of events having caused unlawful disclosure of information. The filed is to be filled in, where the field  "Description of computer incident" has insufficient information about unlawful  disclosure of PD |
| 27 | Characteristics of PD | Text field | Information characterising unlawfully disclosed PD shall be specified, including the type of the subject whose PD were disclosed, the structure of unlawfully disclosed PD, the number and relevance of entries etc. |
| 28 | Supposed damage caused to the PD subjects' rights | Text field | Description of supposed damage which may be caused to the subjects upon use of unlawfully disclosed information |
| 29 | Full name of the person authorised by the operator to interact  with Roskomnadzor  on the incident | Text field | - |
| 30 | Mobile telephone of the person authorised to interact  with Roskomnadzor  on the incident | In accordance with the Russian numbering system and plan | - |
| 31 | E-mail address for sending information about notification | In the format  of e-mail address | - |
| 32 | Assessment of consequences of computer incident | Impact on confidentiality | CO | In case the specified consequences have occurred | [High] [Low] | - |
| 33 | Impact on integrity | [High] [Low] | - |
| 34 | Impact on availability | [High] [Low] | - |
| 35 | Measures taken to respond  to computer  incident | Description of acts taken in the process of responding to the computer incident | N | - | Text field | - |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 36 | Relation to other notifications | Type of related notification | CO | To be filled in where the Bank of Russia was previously sent a notification related  to the current notification | [NTF\_OWC] [NTF\_ISI] [NTF\_ORI] [NTF\_CI] [NTF\_CA] [NTF\_VLN] | [NTF\_OWC] - notification   * about identified cases and (or) attempts of funds transfers without consent of the client as well as identified cases   and (or) attempts of carrying out operations aimed at consummation of financial transactions using financial platform, not relying on the financial platform participant's will, [NTF\_ISI] - notification about identification of an information security incident or the findings of investigation of an information security incident [NTF\_ORI] - notification   * about identification of an operational reliability incident or * the findings of investigation of an operational reliability incident   [NTF\_CI] - notification   * about computer incidents [NTF\_CA] - notification * about computer attacks [NTF\_VLN] - notification * about identified vulnerabilities |
| 37 | Type of relation to other notifications | [Preceding event]  [Subsidiary event] [Related event] [Specification of information  about event] | - |
| 38 | Registration number of notification | In accordance with AIPS FinTsERT format | Identifier of notification or response to the request previously sent to FinTsERT by an information exchange participant |
| 39 | Restrictive TLP marker | Restrictive marker for distribution of information from the given notification | N | - | [TLP: WHITE] [TLP: GREEN] [TLP: AMBER] [TLP: RED] | In accordance with designations accepted in TLP protocol  Default value [TLP: GREEN], unless otherwise specified |
| 40 | Necessity of FinTsERT involvement | Necessity of FinTsERT involvement to rectify the consequences of the computer incident | CO | Where necessary | [Yes] | - |

**Data provision form NTF\_CI\_Malware infection - Form of provision of data about a computer incident related to malware infection**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 1 | Type of notification | Type of notification | O | - | [NTF\_CI\_Malware infection] | Pre-filled field |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 2 | Description of computer incident | Description of computer incident | N | - | Text field | Textual description of computer incident (including additional information on the method of CI realisation, method of CI identification etc.). Where a computer incident is identified  using information from the bulletin of the Bank of Russia or NCCCI, the number of such bulletin is to be specified |
| 3 | Classification of computer incident | Vector | O | - | [EXT]  [INT] | [EXT] - targeted  at the client or counterparty of the financial institution ot other persons  cooperating with the financial institution  [INT] - targeted at computer objects  of financial institution |
| 4 | Type of computer incident | O | - | [Malware infection] | Pre-filled field |
| 5 | Date and time of detection | Date and time of computer incident identification | O | - | In accordance with RFC 3339 | Moscow time [UTC +03:00] |
| 6 | Information about facilities being the target of computer incident | Name of controlled information resource | O | - | Text field | - |
| 7 |  | Category of controlled resource | CO | If it is a CII object | [No relevance category]  [Third relevance category] [Second relevance category] [First relevance  category] | - |
| 8 |  | Code of level of attacked object/subject | O | - | From the classifier  "Types of objects and subjects" set forth  in [Appendix 28](#_bookmark67) | - |
| 9 |  | Code of type of attacked object/subject | O | - | The list depends on the field "Code of level of attacked object/subject". | The list depends on the field  "Code of level of attacked object/subject" |
|  |  |  |  |  | From the classifier  "Types of objects and subjects" set forth  in [Appendix 28](#_bookmark67) |  |
| 10 |  | Availability of Internet connection | O | - | [Yes]/[No] | - |
| 11 |  | Country/region | O | - | In ISP-3166-2 format | - |
| 12 |  | IPv6-address of attacked resource | CO | One of the fields must be filled in | List of IP-addresses | - |
| 13 |  | IPv6-address of attacked resource |  |  |  |  |
| 14 |  | Domain name of attacked resource |  |  | List of domain names |  |
| 15 |  | URI-address of attacked resource |  |  | List of URI-addresses |  |
| 16 |  | e-mail address of attacked object |  |  | List of e-mail addresses |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 17 |  | Attacked network service and port/protocol | CO | In case of availability of respective information | Text field | - |
| 18 | Information about objects | IPv6-address of malicious | CO | IPv4-address of | List of IP-addresses | - |
|  | of malicious | object has been identified |  | malicious |  |  |
|  | activity |  |  | object has been identified |  |  |
|  | having caused |  |  |  |  |  |
|  | the computer |  |  |  |  |  |
|  | incident |  |  |  |  |  |
| 19 |  | IPv6-address of a malicious object |  | IPv6-address of a malicious object has been identified |  | - |
| 20 |  | Domain name of malicious object |  | Domain name of malicious object has been identified | List of domain names | - |
| 21 |  | URI-address of malicious object |  | URI-address of malicious object has been identified | List of URI-addresses | - |
| 22 |  | e-mail-address of malicious |  | E-mail-address | List of e-mail addresses | - |
|  |  | object or |  | of malicious |  |  |
|  |  | subject |  | object  or subject has been identified |  |  |
| 23 |  | Name of antivirus | CO | If malware was | Text field | - |
|  |  | having identified malware |  | identified by |  |  |
|  |  | infection |  | antivirus |  |  |
| 24 |  | Description and classification of malicious software | N | - | Text field | - |
| 25 |  | Network activity | CO | In case of availability of | Text field | - |
|  |  |  |  | information about network |  |  |
|  |  |  |  | activity |  |  |
|  |  |  |  | of malware |  |  |
| 26 |  | Vulnerability | CO | Where the fact of | List of used | - |
|  |  |  |  | use of | security vulnerabilities |  |
|  |  |  |  | of vulnerabilities | of software |  |
|  |  |  |  | by malware has been identified | or hardware |  |
|  |  |  |  |  | from the respective |  |
|  |  |  |  |  | catalogue |  |
|  |  |  |  |  | (for instance, CVE, TDB |  |
|  |  |  |  |  | FSTEC etc.) |  |
| 27 |  | Name of system of description of vulnerabilities |  |  | Text field | - |
| 28 |  | Description of vulnerability |  |  | Text field | - |
|  |  | not described in any |  |  |  |  |
|  |  | system of description |  |  |  |  |
|  |  | of vulnerabilities |  |  |  |  |
| 29 |  | Malware file | CO | One | File | - |
|  |  |  |  | of the fields |  |  |
|  |  |  |  | must be filled in |  |  |
| 30 |  | URL for downloading |  |  | Text field | - |
| 31 |  | Hash sum | O | - | Text field | - |
| 32 |  | Hashing algorithm |  | - | [SHA256] | - |
|  |  |  |  |  | [SHA1] |  |
|  |  |  |  |  | [MD5] |  |
| 33 | Information about | Supposed | CO | The block is to be filled in | Text field | Description of events |
|  | unlawful | reasons having caused |  | where the computer |  | having caused unlawful disclosure |
|  | disclosure of PD | violation of PD subjects'  rights |  | incident  resulted in |  | of information. The field  is to be filled in, where the field |
|  |  |  |  | PD |  | "Description of computer |
|  |  |  |  | leak |  | incident" does not contain sufficient |
|  |  |  |  |  |  | information about unlawful |
|  |  |  |  |  |  | disclosure of PD |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 34 |  | Characteristics of PD |  |  | Text field | Information characterising unlawfully disclosed PD shall be specified, including the type of the subject whose PD were disclosed, the structure of unlawfully disclosed PD, the number and relevance of entries etc. |
| 35 | Supposed damage caused to the PD subjects' rights | Text field | Description of supposed damage which may be caused to the subjects upon use of unlawfully disclosed information |
| 36 | Full name of the person authorised by the operator to interact  with Roskomnadzor  on the incident | Text field | - |
| 37 | Mobile telephone of the person authorised to interact  with Roskomnadzor  on the incident | In accordance with the Russian numbering system and plan | - |
| 38 | E-mail address for sending information about notification | In the format  of e-mail address | - |
| 39 | Assessment of consequences of computer incident | Impact on confidentiality | CO | In case the specified consequences have occurred | [High] [Low] | - |
| 40 | Impact on integrity | [High] [Low] | - |
| 41 | Impact on availability | [High] [Low] | - |
| 42 | Measures taken to respond  to computer  incident | Description of acts taken in the process of responding to the computer incident | N | - | Text field | - |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 43 | Relation to other notifications | Type of related notification | CO | To be filled in where the Bank of Russia was previously sent a notification related  to the current notification | [NTF\_OWC] [NTF\_ISI] [NTF\_ORI] [NTF\_CI] [NTF\_CA] [NTF\_VLN] | [NTF\_OWC] - notification   * about identified cases and (or) attempts of funds transfers without consent of the client as well as identified cases   and (or) attempts of carrying out operations aimed at consummation of financial transactions using financial platform, not relying on the financial platform participant's will, [NTF\_ISI] - notification about identification of an information security incident or the findings of investigation of an information security incident [NTF\_ORI] - notification   * about identification of an operational reliability incident or * the findings of investigation of an operational reliability incident   [NTF\_CI] - notification   * about computer incidents [NTF\_CA] - notification * about computer attacks [NTF\_VLN] - notification * about identified vulnerabilities |
| 44 | Type of relation to other notifications | [Preceding event]  [Subsidiary event] [Related event] [Specification of information  about event] | - |
| 45 | Registration number of notification | In accordance with AIPS FinTsERT format | Identifier of notification or response to the request previously sent to FinTsERT by an information exchange participant |
| 46 | Restrictive TLP marker | Restrictive marker for distribution of information from the given notification | N | - | [TLP: WHITE] [TLP: GREEN] [TLP: AMBER] [TLP: RED] | In accordance with designations accepted in TLP protocol.  Default value [TLP: GREEN], unless otherwise specified |
| 47 | Necessity of FinTsERT involvement | Necessity of FinTsERT involvement to rectify the consequences of the computer incident | CO | Where necessary | [Yes] | - |

**Data provision form NTF\_CI\_Account compromise - Form of provision of data about a computer incident related to compromise of account**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 1 | Type of notification | Type of notification | O | - | [NTF\_CI\_Account compromise] | Pre-filled field |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 2 | Description of computer incident | Description of computer incident | N | - | Text field | Textual description of computer incident (including additional information on the method of CI realisation, method of CI identification etc.). Where a computer incident is identified  using information from the bulletin of the Bank of Russia or NCCCI, the number of such bulletin is to be specified |
| 3 | Classification of computer incident | Vector | O | - | [EXT]  [INT] | [EXT] - targeted  at the client or counterparty of the financial institution ot other persons  cooperating with the financial institution  [INT] - targeted at computer objects  of financial institution |
| 4 | Type of computer incident | O | - | [Account compromise] | Pre-filled field |
| 5 | Date and time of detection | Date and time of computer incident identification | O | - | In accordance with RFC 3339 | Moscow time [UTC +03:00] |
| 6 | Information about facilities being the target of computer incident | Name of controlled information resource | O | - | Text field | - |
| 7 |  | Category of controlled resource | CO | If it is a CII object | [No relevance category]  [Third relevance category] [Second relevance category] [First relevance  category] | - |
| 8 |  | Code of level of attacked object/subject | O | - | From the classifier  "Types of objects and subjects" set forth  in [Appendix 28](#_bookmark67) | - |
| 9 |  | Code of type of attacked object/subject | O | - | The list depends on the field "Code of level of attacked object/subject". | The list depends on the field  "Code of level of attacked object/subject" |
|  |  |  |  |  | From the classifier  "Types of objects and subjects" set forth  in [Appendix 28](#_bookmark67) |  |
| 10 |  | Availability of Internet connection | O | - | [Yes]/[No] | - |
| 11 |  | Country/region | O | - | In ISP-3166-2 format | - |
| 12 |  | IPv6-address of attacked resource | CO | One of the fields must be filled in | List of IP-addresses | - |
| 13 |  | IPv6-address of attacked resource |  |  |  |  |
| 14 |  | Domain name of attacked resource |  |  | List of domain names |  |
| 15 |  | URI-address of attacked resource |  |  | List of URI-addresses |  |
| 16 |  | e-mail address of attacked object |  |  | List of e-mail addresses |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 17 |  | Attacked network service and port/protocol | CO | In case of availability of respective information | Text field | - |
| 18 | Information about malicious activity objects having caused the computer incident | IPv4-address of malicious object | CO | IPv4-address of malicious object has been identified | List of IP-addresses | - |
| 19 | IPv6-address of a malicious object | IPv6-address of a malicious object has been identified | - |
| 20 | Domain name of malicious object | Domain name of malicious object has been identified | List of domain names | - |
| 21 | Login of compromised account | O | - | Text field | - |
| 22 | Privileges of compromised account | O | - | Text field | - |
| 23 | Compromise method | CO | In case of availability of respective information | Text field | - |
| 24 | Information about unlawful disclosure of PD | Supposed reasons having caused violation of PD subjects' rights | CO | The block is to be filled in  in case, when the computer incident results in PD leak | Text field | Description of events having caused unlawful disclosure of information. The filed is to be filled in, where the field  "Description of computer incident" has insufficient information about unlawful  disclosure of PD |
| 25 | Characteristics of PD | Text field | Information characterising unlawfully disclosed PD shall be specified, including the type of the subject whose PD were disclosed, the structure of unlawfully disclosed PD, the number and relevance of entries etc. |
| 26 | Supposed damage caused to the PD subjects' rights | Text field | Description of supposed damage which may be caused to the subjects upon use of unlawfully disclosed information |
| 27 | Full name of the person authorised by the operator to interact  with Roskomnadzor  on the incident | Text field | - |
| 28 | Mobile telephone of the person authorised to interact  with Roskomnadzor  on the incident | In accordance with the Russian numbering system and plan | - |
| 29 | E-mail address for sending information about notification | In the format  of e-mail address | - |
| 30 | Assessment of consequences of computer incident | Impact on confidentiality | CO | In case the specified consequences have occurred | [High] [Low] | - |
| 31 | Impact on integrity | [High] [Low] | - |
| 32 | Impact on availability | [High] [Low] | - |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 33 | Measures taken to respond  to computer  incident | Description of acts taken in the process of responding to the computer incident | N | - | Text field | - |
| 34 | Relation to other notifications | Type of related notification | CO | To be filled in where the Bank of Russia was previously sent a notification related  to the current notification | [NTF\_OWC] [NTF\_ISI] [NTF\_ORI] [NTF\_CI] [NTF\_CA] [NTF\_VLN] | [NTF\_OWC] - notification   * about identified cases and (or) attempts of funds transfers without consent of the client as well as identified cases   and (or) attempts of carrying out operations aimed at consummation of financial transactions using financial platform, not relying on the financial platform participant's will, [NTF\_ISI] - notification about identification of an information security incident or the findings of investigation of an information security incident [NTF\_ORI] - notification   * about identification of an operational reliability incident or * the findings of investigation of an operational reliability incident   [NTF\_CI] - notification   * about computer incidents [NTF\_CA] - notification * about computer attacks [NTF\_VLN] - notification * about identified vulnerabilities |
| 35 | Type of relation to other notifications | [Preceding event]  [Subsidiary event] [Related event] [Specification of information  about event] | - |
| 36 | Registration number of notification | In accordance with AIPS FinTsERT format | Identifier of notification or response to the request previously sent to FinTsERT by an information exchange participant |
| 37 | Restrictive TLP marker | Restrictive marker for distribution of information from the given notification | N | - | [TLP: WHITE] [TLP: GREEN] [TLP: AMBER] [TLP: RED] | In accordance with designations accepted in TLP protocol.  Default value [TLP: GREEN], unless otherwise specified |
| 38 | Necessity of FinTsERT involvement | Necessity of FinTsERT involvement to rectify the consequences of the computer incident | CO | Where necessary | [Yes] | - |

**Data provision form NTF\_CI\_Prohibited content - Form of provision of data about a computer incident related to publication on the controlled resource of information prohibited by the legislation of the Russian Federation**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 1 | Type of notification | Type of notification | O | - | [NTF\_CI\_Prohibited content] | Pre-filled field |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 2 | Description of computer incident | Description of computer incident | N | - | Text field | Textual description of computer incident (including additional information on the method of CI realisation, method of CI identification etc.). Where a computer incident is identified  using information from the bulletin of the Bank of Russia or NCCCI, the number of such bulletin is to be specified |
| 3 | Classification of computer incident | Vector | O | - | [INT] | Pre-filled field |
| 4 | Type of computer incident | O | - | [Prohibited content] | Pre-filled field |
| 5 | Date and time of detection | Date and time of computer incident identification | O | - | In accordance with RFC 3339 | Moscow time [UTC +03:00] |
| 6 | Information about facilities being the target of computer incident | Name of controlled information resource | O | - | Text field | - |
| 7 |  | Category of controlled resource | CO | If it is a CII object | [No relevance category]  [Third relevance category] [Second relevance category] [First relevance  category] | - |
| 8 |  | Code of level of attacked object/subject | O | - | From the classifier  "Types of objects and subjects" set forth  in [Appendix 28](#_bookmark67) | - |
| 9 |  | Code of type of attacked object/subject | O | - | The list depends on the field "Code of level of attacked object/subject". | The list depends on the field  "Code of level of attacked object/subject" |
|  |  |  |  |  | From the classifier  "Types of objects and subjects" set forth  in [Appendix 28](#_bookmark67) |  |
| 10 |  | Availability of Internet connection | O | - | [Yes]/[No] | - |
| 11 |  | Country/region | O | - | In ISP-3166-2 format | - |
| 12 |  | IPv6-address of attacked resource | CO | One of the fields must be filled in | List of IP-addresses | - |
| 13 |  | IPv6-address of attacked resource |  |  |  |  |
| 14 |  | Domain name of attacked resource |  |  | List of domain names |  |
| 15 |  | URI-address of attacked resource |  |  | List of URI-addresses |  |
| 16 | Information about malicious activity objects having caused the computer incident | IPv4-address of malicious object | CO | IPv4-address of malicious object has been identified | List of IP-addresses | - |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 17 |  | IPv6-address of a malicious object |  | IPv6-address of a malicious object has been identified |  | - |
| 18 | Domain name of malicious object | Domain name of malicious object has been identified | List of domain names | - |
| 19 | URI-address of malicious object | URI-address of malicious object has been identified | List of URI-addresses | - |
| 20 | Assessment of consequences of computer incident | Impact on confidentiality | CO | In case the specified consequences have occurred | [High] [Low] | - |
| 21 | Impact on integrity | [High] [Low] | - |
| 22 | Impact on availability | [High] [Low] | - |
| 23 | Measures taken to respond  to computer  incident | Description of acts taken in the process of responding to the computer incident | N | - | Text field | - |
| 24 | Relation to other notifications | Type of related notification | CO | To be filled in where the Bank of Russia was previously sent a notification related  to the current notification | [NTF\_OWC] [NTF\_ISI] [NTF\_ORI] [NTF\_CI] [NTF\_CA] [NTF\_VLN] | [NTF\_OWC] - notification   * about identified cases and (or) attempts of funds transfers without consent of the client as well as identified cases   and (or) attempts of carrying out operations aimed at consummation of financial transactions using financial platform, not relying on the financial platform participant's will, [NTF\_ISI] - notification about identification of an information security incident or the findings of investigation of an information security incident [NTF\_ORI] - notification   * about identification of an operational reliability incident or * the findings of investigation of an operational reliability incident   [NTF\_CI] - notification   * about computer incidents [NTF\_CA] - notification * about computer attacks [NTF\_VLN] - notification * about identified vulnerabilities |
| 25 | Type of relation to other notifications | [Preceding event]  [Subsidiary event] [Related event] [Specification of information  about event] | - |
| 26 | Registration number of notification | In accordance with AIPS FinTsERT format | Identifier of notification or response to the request previously sent to FinTsERT by an information exchange participant |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 27 | Restrictive TLP marker | Restrictive marker for distribution of information from the given notification | N | - | [TLP: WHITE] [TLP: GREEN] [TLP: AMBER] [TLP: RED] | In accordance with designations accepted in TLP protocol  Default value [TLP: GREEN], unless otherwise specified |
| 28 | Necessity of FinTsERT involvement | Necessity of FinTsERT involvement to rectify the consequences of the computer incident | CO | Where necessary | [Yes] | - |

**Data provision form NTF\_CI\_Social engineering - Form of provision of data about a computer incident related to Social engineering**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 1 | Type of notification | Type of notification | O | - | [NTF\_CI\_Social engineering] | Pre-filled field |
| 2 | Description of computer incident | Description of computer incident | N | - | Text field | Textual description of computer incident (including additional information on the method of CI realisation, method of CI identification etc.). Where a computer incident is identified  using information from the bulletin of the Bank of Russia or NCCCI, the number of such bulletin is to be specified |
| 3 | Classification of computer incident | Vector | O | - | [EXT]  [INT] | [EXT] - targeted  at the client or counterparty of the financial institution ot other persons  cooperating with the financial institution  [INT] - targeted at computer objects  of financial institution |
| 4 | Type of computer incident | O | - | [Social engineering] | Pre-filled field |
| 5 | Date and time of detection | Date and time of computer incident identification | O | - | In accordance with RFC 3339 | Moscow time [UTC +03:00] |
| 6 | Information about facilities being the target of computer incident | Code of level of attacked object/subject | O | - | [Subject] | Pre-filled field |
| 7 | Code of type of attacked object/subject | O | - | From the classifier  "Types of objects and subjects" set forth in [Appendix 28](#_bookmark67)  [Employee] [Client] [Partner] | - |
| 8 | Information about malicious activity objects having caused the computer incident | IPv4-address of malicious object | CO | IPv4-address of malicious object has been identified | List of IP-addresses | At least one field is to be filled in |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 9 |  | IPv6-address of a malicious object |  | IPv6-address of a malicious object has been identified |  |  |
| 10 | Domain name of malicious object | Domain name of malicious object has been identified | List of domain names |
| 11 | URI-address of malicious object | URI-address of malicious object has been identified | List of URI-addresses |
| 12 | e-mail-address of malicious object or subject | E-mail-address of malicious object or subject has been identified | List of e-mail addresses |
| 13 | Mobile telephone communications subscriber's number of malicious subject | Mobile telephone communications subscriber's number of malicious subject has been identified | List of numbers in accordance with the Russian numbering system and plan |
| 14 | Interaction channel | O | - | [Telephone call] [SMS]  [E-mail] [Instant messaging system] [Website]  [Other channel] | - |
| 15 | Message text | CO | "Interaction channel" = { [SMS], [E-mail], [Instant messaging system]} | Text field or txt-file | - |
| 16 | Assessment of consequences of computer incident | Impact on confidentiality | CO | In case the specified consequences have occurred | [High] [Low] | - |
| 17 | Impact on integrity | [High] [Low] | - |
| 18 | Impact on availability | [High] [Low] | - |
| 19 | Measures taken to respond  to computer  incident | Description of acts taken in the process of responding to the computer incident | N | - | Text field | - |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 20 | Relation to other notifications | Type of related notification | CO | To be filled in where the Bank of Russia was previously sent a notification related  to the current notification | [NTF\_OWC] [NTF\_ISI] [NTF\_ORI] [NTF\_CI] [NTF\_CA] [NTF\_VLN] | [NTF\_OWC] - notification   * about identified cases and (or) attempts of funds transfers without consent of the client as well as identified cases   and (or) attempts of carrying out operations aimed at consummation of financial transactions using financial platform, not relying on the financial platform participant's will, [NTF\_ISI] - notification about identification of an information security incident or the findings of investigation of an information security incident [NTF\_ORI] - notification   * about identification of an operational reliability incident or * the findings of investigation of an operational reliability incident   [NTF\_CI] - notification   * about computer incidents [NTF\_CA] - notification * about computer attacks [NTF\_VLN] - notification * about identified vulnerabilities |
| 21 | Type of relation to other notifications | [Preceding event]  [Subsidiary event] [Related event] [Specification of information  about event] | - |
| 22 | Registration number of notification | In accordance with AIPS FinTsERT format | Identifier of notification or response to the request previously sent to FinTsERT by an information exchange participant |
| 23 | Restrictive TLP marker | Restrictive marker for distribution of information from the given notification | N | - | [TLP: WHITE] [TLP: GREEN] [TLP: AMBER] [TLP: RED] | In accordance with designations accepted in TLP protocol.  Default value [TLP: GREEN], unless otherwise specified |
| 24 | Necessity of FinTsERT involvement | Necessity of FinTsERT involvement to rectify the consequences of the computer incident | CO | Where necessary | [Yes] | - |

**Data provision form NTF\_CI\_Traffic hijacking - Form of provision of data about a computer incident related to capture of network traffic**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 1 | Type of notification | Type of notification | O | - | [NTF\_CI\_Traffic hijacking] | Pre-filled field |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 2 | Description of computer incident | Description of computer incident | N | - | Text field | Textual description of computer incident (including additional information on the method of CI realisation, method of CI identification etc.). Where a computer incident is identified  using information from the bulletin of the Bank of Russia or NCCCI, the number of such bulletin is to be specified |
| 3 | Classification of computer incident | Vector | O | - | [INT] | Pre-filled field |
| 4 | Type of computer incident | O | - | [Traffic hijacking] | Pre-filled field |
| 5 | Date and time of detection | Date and time of computer incident identification | O | - | In accordance with RFC 3339 | Moscow time [UTC +03:00] |
| 6 | Information about facilities being the target of computer incident | Name of controlled information resource | O | - | Text field | - |
| 7 |  | Category of controlled resource | CO | If it is a CII object | [No relevance category]  [Third relevance category] [Second relevance category] [First relevance  category] | - |
| 8 |  | Code of level of attacked object/subject | O | - | From the classifier  "Types of objects and subjects" set forth  in [Appendix 28](#_bookmark67) | - |
| 9 |  | Code of type of attacked object/subject | O | - | The list depends on the field "Code of level of attacked object/subject". | The list depends on the field  "Code of level of attacked object/subject" |
|  |  |  |  |  | From the classifier  "Types of objects and subjects" set forth  in [Appendix 28](#_bookmark67) |  |
| 10 |  | Availability of Internet connection | O | - | [Yes]/[No] | - |
| 11 |  | Country/region | O | - | In ISP-3166-2 format | - |
| 12 |  | AS-Path to the attacked autonomous system (ASN) |  |  | Text field |  |
| 13 | Information about malicious activity objects having caused the computer incident | Number of dummy autonomous system (ASN) | O | - | Text field | - |
| 14 | AS name | O | - | Text field | - |
| 15 | LIR name | O | - | Text field | - |
| 16 | Reference to Looking Glass | CO | In case of availability of | Text field | - |
| 17 | Authentic prefix | N | - | Text field | - |
| 18 | Dummy prefix | N | - | Text field | - |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 19 | Assessment of consequences of computer incident | Impact on confidentiality | CO | In case the specified consequences have occurred | [High] [Low] | - |
| 20 | Impact on integrity | [High] [Low] | - |
| 21 | Impact on availability | [High] [Low] | - |
| 22 | Measures taken to respond  to computer  incident | Description of acts taken in the process of responding to the computer incident | N | - | Text field | - |
| 23 | Relation to other notifications | Type of related notification | CO | To be filled in where the Bank of Russia was previously sent a notification related  to the current notification | [NTF\_OWC] [NTF\_ISI] [NTF\_ORI] [NTF\_CI] [NTF\_CA] [NTF\_VLN] | [NTF\_OWC] - notification   * about identified cases and (or) attempts of funds transfers without consent of the client as well as identified cases   and (or) attempts of carrying out operations aimed at consummation of financial transactions using financial platform, not relying on the financial platform participant's will, [NTF\_ISI] - notification about identification of an information security incident or the findings of investigation of an information security incident [NTF\_ORI] - notification   * about identification of an operational reliability incident or * the findings of investigation of an operational reliability incident   [NTF\_CI] - notification   * about computer incidents [NTF\_CA] - notification * about computer attacks [NTF\_VLN] - notification * about identified vulnerabilities |
| 24 | Type of relation to other notifications | [Preceding event]  [Subsidiary event] [Related event] [Specification of information  about event] | - |
| 25 | Registration number of notification | In accordance with AIPS FinTsERT format | Identifier of notification or response to the request previously sent to FinTsERT by an information exchange participant |
| 26 | Restrictive TLP marker | Restrictive marker for distribution of information from the given notification | N | - | [TLP: WHITE] [TLP: GREEN] [TLP: AMBER] [TLP: RED] | In accordance with designations accepted in TLP protocol.  Default value [TLP: GREEN], unless otherwise specified |
| 27 | Necessity of FinTsERT involvement | Necessity of FinTsERT involvement to rectify the consequences of the computer incident | CO | Where necessary | [Yes] | - |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |

**Data provision form NTF\_CI\_Unauthorised modification - Form of provision of data about a computer incident related to unauthorised modification of information**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 1 | Type of notification | Type of notification | O | - | [NTF\_CI\_Unauthorised modification] | Pre-filled field |
| 2 | Description of computer incident | Description of computer incident | N | - | Text field | Textual description of computer incident (including additional information on the method of CI realisation, method of CI identification etc.). Where a computer incident is identified  using information from the bulletin of the Bank of Russia or NCCCI, the number of such bulletin is to be specified |
| 3 | Classification of computer incident | Vector | O | - | [INT] | Pre-filled field |
| 4 | Type of computer incident | O | - | [Unauthorised modification] | Pre-filled field |
| 5 | Date and time of detection | Date and time of computer incident identification | O | - | In accordance with RFC 3339 | Moscow time [UTC +03:00] |
| 6 | Information about facilities being the target of computer incident | Name of controlled information resource | O | - | Text field | - |
| 7 | Category of controlled resource | CO | If it is a CII object | [No relevance category]  [Third relevance category] [Second relevance category] [First relevance  category] | - |
| 8 | Code of level of attacked object/subject | O | - | From the classifier  "Types of objects and subjects" set forth  in [Appendix 28](#_bookmark67) | - |
| 9 | Code of type of attacked object/subject | O | - | The list depends on the field "Code of level of attacked object/subject".  From the classifier  "Types of objects and subjects" set forth  in [Appendix 28](#_bookmark67) | The list depends on the field  "Code of level of attacked object/subject" |
| 10 | Availability of Internet connection | O | - | [Yes]/[No] | - |
| 11 | Country/region | O | - | In ISP-3166-2 format | - |
| 12 | IPv6-address of attacked resource | CO | One of the fields must be filled in | List of IP-addresses | - |
| 13 | IPv6-address of attacked resource |
| 14 | Domain name of attacked resource | List of domain names |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 15 |  | URI-address of attacked resource |  |  | List of URI-addresses |  |
| 16 | Attacked network service and port/protocol | CO | In case of availability of respective information | Text field | - |
| 17 | Information about malicious activity objects having caused the computer incident | IPv4-address of malicious object | CO | IPv4-address of malicious object has been identified | List of IP-addresses | - |
| 18 | IPv6-address of a malicious object | IPv6-address of a malicious object has been identified | - |
| 19 | Domain name of malicious object | Domain name of malicious object has been identified | List of domain names | - |
| 20 | URI-address of malicious object | URI-address of malicious object has been identified | List of URI-addresses | - |
| 21 | Assessment of consequences of computer incident | Impact on confidentiality | CO | In case the specified consequences have occurred | [High] [Low] | - |
| 22 | Impact on integrity | [High] [Low] | - |
| 23 | Impact on availability | [High] [Low] | - |
| 24 | Measures taken to respond  to computer  incident | Description of acts taken in the process of responding to the computer incident | N | - | Text field | - |
| 25 | Relation to other notifications | Type of related notification | CO | To be filled in where the Bank of Russia was previously sent a notification related  to the current notification | [NTF\_OWC] [NTF\_ISI] [NTF\_ORI] [NTF\_CI] [NTF\_CA] [NTF\_VLN] | [NTF\_OWC] - notification   * about identified cases and (or) attempts of funds transfers without consent of the client as well as identified cases   and (or) attempts of carrying out operations aimed at consummation of financial transactions using financial platform, not relying on the financial platform participant's will, [NTF\_ISI] - notification about identification of an information security incident or the findings of investigation of an information security incident [NTF\_ORI] - notification   * about identification of an operational reliability incident or * the findings of investigation of an operational reliability incident   [NTF\_CI] - notification   * about computer incidents [NTF\_CA] - notification * about computer attacks [NTF\_VLN] - notification * about identified vulnerabilities |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 26 |  | Type of relation to other notifications |  |  | [Preceding event]  [Subsidiary event] [Related event] [Specification of information  about event] | - |
| 27 | Registration number of notification | In accordance with AIPS FinTsERT format | Identifier of notification or response to the request previously sent to FinTsERT by an information exchange participant |
| 28 | Restrictive TLP marker | Restrictive marker for distribution of information from the given notification | N | - | [TLP: WHITE] [TLP: GREEN] [TLP: AMBER] [TLP: RED] | In accordance with designations accepted in TLP protocol.  Default value [TLP: GREEN], unless otherwise specified |
| 29 | Necessity of FinTsERT involvement | Necessity of FinTsERT involvement to rectify the consequences of the computer incident | CO | Where necessary | [Yes] | - |

**Data provision form NTF\_CI\_Unauthorised access - Form of provision of data about a computer incident related to unauthorised disclosure of information**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 1 | Type of notification | Type of notification | O | - | [NTF\_CI\_Unauthorised access] | Pre-filled field |
| 2 | Description of computer incident | Description of computer incident | N | - | Text field | Textual description of computer incident (including additional information on the method of CI realisation, method of CI identification etc.). Where a computer incident is identified  using information from the bulletin of the Bank of Russia or NCCCI, the number of such bulletin is to be specified |
| 3 | Classification of computer incident | Vector | O | - | [INT] | Pre-filled field |
| 4 | Type of computer incident | O | - | [Unauthorised access] | Pre-filled field |
| 5 | Date and time of detection | Date and time of computer incident identification | O | - | In accordance with RFC 3339 | Moscow time [UTC +03:00] |
| 6 | Information about facilities being the target of computer incident | Name of controlled information resource | O | - | Text field | - |
| 7 | Category of controlled resource | CO | If it is a CII object | [No relevance category]  [Third relevance category] [Second relevance category] [First relevance  category] | - |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 8 |  | Code of level of attacked object/subject | O | - | From the classifier  "Types of objects and subjects" set forth  in [Appendix 28](#_bookmark67) | - |
| 9 | Code of type of attacked object/subject | O | - | The list depends on the field "Code of level of attacked object/subject". | The list depends on the field  "Code of level of attacked object/subject" |
|  |  |  |  | From the classifier  "Types of objects and subjects" set forth  in [Appendix 28](#_bookmark67) |  |
| 10 | Availability of Internet connection | O | - | [Yes]/[No] | - |
| 11 | Country/region | O | - | In ISP-3166-2 format | - |
| 12 | IPv6-address of attacked resource | CO | One of the fields must be filled in | List of IP-addresses | - |
| 13 | IPv6-address of attacked resource |  |  |  |  |
| 14 | Domain name of attacked resource |  |  | List of domain names |  |
| 15 | URI-address of attacked resource |  |  | List of URI-addresses |  |
| 16 | e-mail address of attacked object |  |  | List of e-mail addresses |  |
| 17 | Attacked network service and port/protocol | CO | In case of availability of respective information | Text field | - |
| 18 | Information about malicious activity objects having caused the computer incident | IPv4-address of malicious system | CO | IPv4-address of malicious system or object has been identified | List of IP-addresses | - |
| 19 | IPv6-address of malicious system | IPv6-address of malicious system or object has been identified | - |
| 20 | Domain name of malicious system | Domain name of malicious system of object has been identified | List of domain names | - |
| 21 | e-mail-address of malicious object | E-mail-address of malicious system or object has been identified | List of e-mail addresses | - |
| 22 | Information about unlawful disclosure of PD | Supposed reasons having caused violation of PD subjects' rights | CO | The block is to be filled in  in case, when the computer incident results in PD leak | Text field | Description of events having caused unlawful disclosure of information. The filed is to be filled in, where the field  "Description of computer incident" has insufficient information about unlawful  disclosure of PD |
| 23 | Characteristics of PD | Text field | Information characterising unlawfully disclosed PD shall be specified, including the type of the subject whose PD were disclosed, the structure of unlawfully disclosed PD, the number and relevance of entries etc. |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 24 |  | Supposed damage caused to the PD subjects' rights |  |  | Text field | Description of supposed damage which may be caused to the subjects upon use of unlawfully disclosed information |
| 25 | Full name of the person authorised by the operator to interact  with Roskomnadzor  on the incident | Text field | - |
| 26 | Mobile telephone of the person authorised to interact  with Roskomnadzor  on the incident | In accordance with the Russian numbering system and plan | - |
| 27 | E-mail address for sending information about notification | In the format of e-mail-address | - |
| 28 | Assessment of consequences of computer incident | Impact on confidentiality | CO | In case the specified consequences have occurred | [High] [Low] | - |
| 29 | Impact on integrity | [High] [Low] | - |
| 30 | Impact on availability | [High] [Low] | - |
| 31 | Measures taken to respond  to computer  incident | Description of acts taken in the process of responding to the computer incident | N | - | Text field | - |
| 32 | Relation to other notifications | Type of related notification | CO | To be filled in where the Bank of Russia was previously sent a notification related  to the current notification | [NTF\_OWC] [NTF\_ISI] [NTF\_ORI] [NTF\_CI] [NTF\_CA] [NTF\_VLN] | [NTF\_OWC] - notification   * about identified cases and (or) attempts of funds transfers without consent of the client as well as identified cases   and (or) attempts of carrying out operations aimed at consummation of financial transactions using financial platform, not relying on the financial platform participant's will, [NTF\_ISI] - notification about identification of an information security incident or the findings of investigation of an information security incident [NTF\_ORI] - notification   * about identification of an operational reliability incident or * the findings of investigation of an operational reliability incident   [NTF\_CI] - notification   * about computer incidents [NTF\_CA] - notification * about computer attacks [NTF\_VLN] - notification * about identified vulnerabilities |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 33 |  | Type of relation to other notifications |  |  | [Preceding event]  [Subsidiary event] [Related event] [Specification of information  about event] | - |
| 34 | Registration number of notification | In accordance with AIPS FinTsERT format | Identifier of notification or response to the request previously sent to FinTsERT by an information exchange participant |
| 35 | Restrictive TLP marker | Restrictive marker for distribution of information from the given notification | N | - | [TLP: WHITE] [TLP: GREEN] [TLP: AMBER] [TLP: RED] | In accordance with designations accepted in TLP protocol.  Default value [TLP: GREEN], unless otherwise specified |
| 36 | Necessity of FinTsERT involvement | Necessity of FinTsERT involvement to rectify the consequences of the computer incident | CO | Where necessary | [Yes] | - |

**Data provision form NTF\_CI\_SIM - Form of provision of data about a computer incident related to change (spoofing) of a mobile subscriber identifier (IMSI), mobile equipment identifier (IMEI) or a SIM-card**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 1 | Type of notification | Type of notification | O | - | [NTF\_CI\_SIM] | Pre-filled field |
| 2 | Description of computer incident | Description of computer incident | N | - | Text field | Textual description of computer incident (including additional information on the method of CI realisation, method of CI identification etc.). Where a computer incident is identified  using information from the bulletin of the Bank of Russia or NCCCI, the number of such bulletin is to be specified |
| 3 | Classification of computer incident | Vector | O | - | [EXT] | Pre-filled field |
| 4 | Type of computer incident | O | - | [SIM] | Pre-filled field |
| 5 | Date and time of detection | Date and time of computer incident identification | O | - | In accordance with RFC 3339 | Moscow time [UTC +03:00] |
| 6 | Information about malicious activity objects having caused the computer incident | Mobile telephone communications subscriber's number | O | - | In accordance with the Russian numbering system and plan | - |
| 7 | IMSI | O | - | Text field | - |
| 8 | Communications provider | N | - | Text field | - |
| 9 | Date of IMSI change | N | - | Text field | - |
| 10 | Assessment of consequences of computer incident | Impact on confidentiality | CO | In case the specified consequences have occurred | [High] [Low] | - |
| 11 | Impact on integrity | [High] [Low] | - |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 12 |  | Impact on availability |  |  | [High] [Low] | - |
| 13 | Measures taken to respond  to computer  incident | Description of acts taken in the process of responding to the computer incident | N | - | Text field | - |
| 14 | Relation to other notifications | Type of related notification | CO | To be filled in where the Bank of Russia was previously sent a notification related  to the current notification | [NTF\_OWC] [NTF\_ISI] [NTF\_ORI] [NTF\_CI] [NTF\_CA] [NTF\_VLN] | [NTF\_OWC] - notification   * about identified cases and (or) attempts of funds transfers without consent of the client as well as identified cases   and (or) attempts of carrying out operations aimed at consummation of financial transactions using financial platform, not relying on the financial platform participant's will, [NTF\_ISI] - notification about identification of an information security incident or the findings of investigation of an information security incident [NTF\_ORI] - notification   * about identification of an operational reliability incident or * the findings of investigation of an operational reliability incident   [NTF\_CI] - notification   * about computer incidents [NTF\_CA] - notification * about computer attacks [NTF\_VLN] - notification * about identified vulnerabilities |
| 15 | Type of relation to other notifications | [Preceding event]  [Subsidiary event] [Related event] [Specification of information  about event] | - |
| 16 | Registration number of notification | In accordance with AIPS FinTsERT format | Identifier of notification or response to the request previously sent to FinTsERT by an information exchange participant |
| 17 | Restrictive TLP marker | Restrictive marker for distribution of information from the given notification | N | - | [TLP: WHITE] [TLP: GREEN] [TLP: AMBER] [TLP: RED] | In accordance with designations accepted in TLP protocol.  Default value [TLP: GREEN], unless otherwise specified |
| 18 | Necessity of FinTsERT involvement | Necessity of FinTsERT involvement to rectify the consequences of the computer incident | CO | Where necessary | [Yes] | - |

**Data provision form Attack\_using\_resource - Form of provision of data about a computer incident related to use of controlled resource for attacks**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 1 | Type of notification | Type of notification | O | - | [NTF\_CI\_Attack\_using\_ resource] | Pre-filled field |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 2 | Description of computer incident | Description of computer incident | N | - | Text field | Textual description of computer incident (including additional information on the method of CI realisation, method of CI identification etc.). Where a computer incident is identified  using information from the bulletin of the Bank of Russia or NCCCI, the number of such bulletin is to be specified |
| 3 | Classification of computer incident | Vector | O | - | [INT] | Pre-filled field |
| 4 | Type of computer incident | O | - | [Attack using resource] | Pre-filled field |
| 5 | Date and time of detection | Date and time of computer incident identification | O | - | In accordance with RFC 3339 | Moscow time [UTC +03:00] |
| 6 | Information about objects | Name of controlled | O | - | Text field | - |
|  | being | resource |  |  |  |  |
|  | the target of |  |  |  |  |  |
|  | the computer |  |  |  |  |  |
|  | incident |  |  |  |  |  |
| 7 |  | Category of controlled resource | CO | If it is a CII object | [No relevance category] | - |
|  |  |  |  |  | [Third relevance |  |
|  |  |  |  |  | category] |  |
|  |  |  |  |  | [Second relevance |  |
|  |  |  |  |  | category] |  |
|  |  |  |  |  | [First relevance |  |
|  |  |  |  |  | category] |  |
| 8 |  | Code of level of object/subject | O | - | From the classifier  "Types of objects and subjects" | - |
|  |  |  |  |  | set forth |  |
|  |  |  |  |  | in [Appendix 28](#_bookmark67) |  |
| 9 |  | Code of type of object/subject | O | - | The list depends on the field "Code of level | - |
|  |  |  |  |  | of attacked object/ |  |
|  |  |  |  |  | subject". |  |
|  |  |  |  |  | From the classifier |  |
|  |  |  |  |  | "Types of objects and subjects" |  |
|  |  |  |  |  | set forth |  |
|  |  |  |  |  | in [Appendix 28](#_bookmark67) |  |
| 10 |  | Availability of Internet connection | O | - | [Yes] | Pre-filled field |
| 11 |  | Country/region | O | - | In ISP-3166-2 format | - |
| 12 |  | IPv4-address of controlled resource | CO | One of the fields must be filled in | List of IP-addresses | - |
| 13 |  | IPv6-address of controlled resource |  |  |  |  |
| 14 |  | Domain name of controlled resource |  |  | List of domain names |  |
| 15 |  | URI-address of controlled resource |  |  | List of URI-addresses |  |
| 16 |  | e-mail address of controlled object |  |  | List of e-mail addresses |  |
| 17 |  | Attacked network service and port/protocol | CO | In case of availability of respective information | Text field | - |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 18 | Information about malicious activity objects having caused the computer incident | IPv4-address of malicious object | CO | IPv4-address of malicious object has been identified | List of IP-addresses | - |
| 19 | IPv6-address of a malicious object | IPv6-address of a malicious object has been identified | - |
| 20 | Domain name of malicious object | Domain name of malicious object has been identified | List of domain names | - |
| 21 | URI-address of malicious object | URI-address of malicious object has been identified | List of URI-addresses | - |
| 22 | e-mail-address of malicious object or subject | E-mail-address of malicious object or subject has been identified | List of e-mail addresses | - |
| 23 | Vulnerability | CO | In case the identified vulnerability is described in any system of description of vulnerabilities | List of used vulnerabilities of security of software or hardware, from the respective catalogue (for instance, CVE, TDB FSTEC etc.) | One of blocks must be filled in |
| 24 | Name of system of description of vulnerabilities | Text field |
| 25 | Description of vulnerability | CO | In case the identified vulnerability is not described in any system of description of vulnerabilities | Text field |
| 26 | Description of computer object, in which vulnerability was used | O | - | In the format consistent with the recommendations of the Bank of Russia published on the official website | - |
| 27 | Malware file | CO | One of the fields must be filled in | File | - |
| 28 | URL for downloading | Text field | - |
| 29 | Hash sum | O | - | Text field | - |
| 30 | Hashing algorithm |  | - | [SHA256] [SHA1]  [MD5] | - |
| 31 | Assessment of consequences of computer incident | Impact on confidentiality | CO | In case the specified consequences have occurred | [High] [Low] | - |
| 32 | Impact on integrity | [High] [Low] | - |
| 33 | Impact on availability | [High] [Low] | - |
| 34 | Measures taken to respond  to computer  incident | Description of acts taken in the process of responding to the computer incident | N | - | Text field | - |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 35 | Relation to other notifications | Type of related notification | CO | To be filled in where the Bank of Russia was previously sent a notification related  to the current notification | [NTF\_OWC] [NTF\_ISI] [NTF\_ORI] [NTF\_CI] [NTF\_CA] [NTF\_VLN] | [NTF\_OWC] - notification   * about identified cases and (or) attempts of funds transfers without consent of the client as well as identified cases   and (or) attempts of carrying out operations aimed at consummation of financial transactions using financial platform, not relying on the financial platform participant's will, [NTF\_ISI] - notification about identification of an information security incident or the findings of investigation of an information security incident [NTF\_ORI] - notification   * about identification of an operational reliability incident or * the findings of investigation of an operational reliability incident   [NTF\_CI] - notification   * about computer incidents [NTF\_CA] - notification * about computer attacks [NTF\_VLN] - notification * about identified vulnerabilities |
| 36 | Type of relation to other notifications | [Preceding event]  [Subsidiary event] [Related event] [Specification of information  about event] | - |
| 37 | Registration number of notification | In accordance with AIPS FinTsERT format | Identifier of notification or response to the request previously sent to FinTsERT by an information exchange participant |
| 38 | Restrictive TLP marker | Restrictive marker for distribution of information from the given notification | N | - | [TLP: WHITE] [TLP: GREEN] [TLP: AMBER] [TLP: RED] | In accordance with designations accepted in TLP protocol.  Default value [TLP: GREEN], unless otherwise specified |
| 39 | Necessity of FinTsERT involvement | Necessity of FinTsERT involvement to rectify the consequences of the computer incident | CO | Where necessary | [Yes] | - |

**Data provision form NTF\_CI\_Without\_attack - Form of provision of data about a computer incident not related to computer attack**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 1 | Type of notification | Type of notification | O | - | [NTF\_CI\_Without\_attack] | Pre-filled field |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 2 | Description of computer incident | Description of computer incident | N | - | Text field | Textual description of computer incident (including additional information on the method of CI realisation, method of CI identification etc.). Where a computer incident is identified  using information from the bulletin of the Bank of Russia or NCCCI, the number of such bulletin is to be specified |
| 3 | Classification of computer incident | Vector | O | - | [INT] | Pre-filled field |
| 4 | Type of computer incident | O | - | [Without\_attack] | Pre-filled field |
| 5 | Date and time of detection | Date and time of computer incident identification | O | - | In accordance with RFC 3339 | Moscow time [UTC +03:00] |
| 6 | Information about objects | Name of controlled | O | - | Text field | - |
|  | being | resource |  |  |  |  |
|  | the target of |  |  |  |  |  |
|  | the computer |  |  |  |  |  |
|  | incident |  |  |  |  |  |
| 7 |  | Category of controlled resource | CO | If it is a CII object | [No relevance category] | - |
|  |  |  |  |  | [Third relevance |  |
|  |  |  |  |  | category] |  |
|  |  |  |  |  | [Second relevance |  |
|  |  |  |  |  | category] |  |
|  |  |  |  |  | [First relevance |  |
|  |  |  |  |  | category] |  |
| 8 |  | Code of level of object/subject | O | - | From the classifier  "Types of objects and subjects" | - |
|  |  |  |  |  | set forth |  |
|  |  |  |  |  | in [Appendix 28](#_bookmark67) |  |
| 9 |  | Code of type of object/subject | O | - | The list depends on the field "Code of level | - |
|  |  |  |  |  | of attacked object/ |  |
|  |  |  |  |  | subject". |  |
|  |  |  |  |  | From the classifier |  |
|  |  |  |  |  | "Types of objects and subjects" |  |
|  |  |  |  |  | set forth |  |
|  |  |  |  |  | in [Appendix 28](#_bookmark67) |  |
| 10 |  | Availability of Internet connection | O | - | [Yes]/[No] | - |
| 11 |  | Country/region | O | - | In ISP-3166-2 format | - |
| 12 |  | IPv4-address of controlled resource | CO | One of the fields must be filled in | List of IP-addresses | - |
| 13 |  | IPv6-address of controlled resource |  |  |  |  |
| 14 |  | Domain name of controlled resource |  |  | List of domain names |  |
| 15 |  | URI-address of controlled resource |  |  | List of URI-addresses |  |
| 16 |  | e-mail address of controlled object |  |  | List of e-mail addresses |  |
| 17 | Assessment of consequences of computer incident | Impact on confidentiality | CO | In case the specified consequences have occurred | [High] [Low] | - |
| 18 | Impact on integrity | [High] [Low] | - |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 19 |  | Impact on availability |  |  | [High] [Low] | - |
| 20 | Measures taken to respond  to computer  incident | Description of acts taken in the process of responding to the computer incident | N | - | Text field | - |
| 21 | Relation to other notifications | Type of related notification | CO | To be filled in where the Bank of Russia was previously sent a notification related  to the current notification | [NTF\_OWC] [NTF\_ISI] [NTF\_ORI] [NTF\_CI] [NTF\_CA] [NTF\_VLN] | [NTF\_OWC] - notification   * about identified cases and (or) attempts of funds transfers without consent of the client as well as identified cases   and (or) attempts of carrying out operations aimed at consummation of financial transactions using financial platform, not relying on the financial platform participant's will, [NTF\_ISI] - notification about identification of an information security incident or the findings of investigation of an information security incident [NTF\_ORI] - notification   * about identification of an operational reliability incident or * the findings of investigation of an operational reliability incident   [NTF\_CI] - notification   * about computer incidents [NTF\_CA] - notification * about computer attacks [NTF\_VLN] - notification * about identified vulnerabilities |
| 22 | Type of relation to other notifications | [Preceding event]  [Subsidiary event] [Related event] [Specification of information  about event] | - |
| 23 | Registration number of notification | In accordance with AIPS FinTsERT format | Identifier of notification or response to the request previously sent to FinTsERT by an information exchange participant |
| 24 | Restrictive TLP marker | Restrictive marker for distribution of information from the given notification | N | - | [TLP: WHITE] [TLP: GREEN] [TLP: AMBER] [TLP: RED] | In accordance with designations accepted in TLP protocol.  Default value [TLP: GREEN], unless otherwise specified |
| 25 | Necessity of FinTsERT involvement | Necessity of FinTsERT involvement to rectify the consequences of the computer incident | CO | Where necessary | [Yes] | - |

APPENDIX 21. DATA PROVISION FORM NTF\_CA - FORM OF

PROVISION BY INFORMATION EXCHANGE PARTICIPANTS OF DATA ABOUT COMPUTER ATTACKS

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 1 | Type of notification | Type of notification | O | - | [NTF\_CA] | Pre-filled field |
| 2 | Description of computer attack | Description of computer attack | N | - | Text field | Textual description of computer attack (including additional information  about CA realisation method, CA identification method etc.). Where a computer attack is identified  using information from the bulletin of the Bank of Russia or NCCCI, the number of such bulletin  is to be specified |
| 3 | Classification of computer attack | Vector of computer attack | O | - | [EXT]  [INT] | In accordance with the classifier of computer attacks set forth in [Appendix](#_bookmark38) [18](#_bookmark38) |
| 4 | Type of computer attack | O | - | [DoS]  [Exploit attempt] [Infection attempt] [Login attempt] [Phishing]  [Social engineering]  [Scanning] | In accordance with the classifier of computer attacks set forth in [Appendix](#_bookmark38) [18](#_bookmark38) |
| 5 | Date | Date as of which data about computer attacks are aggregated | O | - | In accordance with RFC 3339 | Moscow time [UTC +03:00] |
| 6 | Information about CII  facilities being the target of computer attacks | Name of controlled information resource | CO | To be filled in where attacks affecting a CII facility are identified | Text field | - |
| 7 | Category of controlled resource | [No relevance category]  [Third relevance category] [Second relevance category] [First relevance  category] | - |
| 8 | Country/region | In ISP-3166-2 format | - |
| 9 | IPv6-address of attacked resource | List of IP-addresses or file | One of the fields must be filled in |
| 10 | IPv6-address of attacked resource |
| 11 | Domain name of attacked resource | List of domain names or file |
| 12 | URI-address of attacked resource | List of URI-addresses or file |
| 13 | e-mail address of attacked object | List of e-mail addresses or file |
| 14 | Attacked network service and port/protocol | Text field | To be filled in where information is available |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 15 | Information about malicious activity objects or subjects | Dataset | CO | The structure of data depends on the field "Type of computer attack" and is specified in the tab "Information about MA objects" | | |
| 16 | Restrictive TLP marker | Restrictive marker for distribution of information from the given notification | N | - | [TLP: WHITE] [TLP: GREEN] [TLP: AMBER] [TLP: RED] | In accordance with designations accepted in TLP protocol.  Default value [TLP: GREEN], unless otherwise specified |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name of computer attack** | **Information about malicious activity objects or subjects** | | | | |
| **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| "DoS (denial of service) attack" | IPv4-address of malicious object | CO | IPv4-address of malicious object has been identified | List of IP-addresses or file | At least one of the fields is to be filled in  All the identified sources of malicious activity in the period of data aggregation are specified |
|  | IPv6-address of a malicious object |  | IPv6-address of a malicious object has been identified |  |  |
|  | Domain name of malicious object |  | Domain name of malicious object has been identified | List of domain names or file |  |
|  | Number of unique "denial of service" attacks (for the combination source of attack + attacked  system)  for the period of data aggregation | O | - | Number | - |
| Attempted use of vulnerability | IPv4-address of malicious object | CO | IPv4-address of malicious object has been identified | List of IP-addresses or file | At least one of the fields is to be filled in  All the identified sources of malicious activity in the period of data aggregation are specified |
|  | IPv6-address of a malicious object |  | IPv6-address of a malicious object has been identified |  |  |
|  | Domain name of malicious object |  | Domain name of malicious object has been identified | List of domain names or file |  |
|  | URI-address of malicious object |  | URI-address of malicious object has been identified | List of URI-addresses or file |  |
|  | e-mail-address of malicious object or subject |  | E-mail-address of malicious object or subject has been identified | List of e-mail addresses or file |  |
|  | List of vulnerabilities being the subject of their attempted use | CO | In case the identified vulnerability is described in any system of description of vulnerabilities | List of used vulnerabilities of security of software or hardware, from the respective catalogue (for instance, CVE, TDB FSTEC etc.) | One of blocks must be filled in |
|  | Name of system of description of vulnerabilities |  |  | Text field |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name of computer attack** | **Information about malicious activity objects or subjects** | | | | |
| **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
|  | Description of vulnerabilities | CO | In case the identified vulnerability is not described in any system of description of vulnerabilities | Text field |  |
| Number of unique attempts of use (for the combination source of attack + attacked system) for the period of data aggregation | O | - | Number | - |
| Attempted deployment of malware modules | IPv4-address of malicious object | CO | IPv4-address of malicious object has been identified | List of IP-addresses or file | All the identified sources of malicious activity in the period of data aggregation are specified |
|  | IPv6-address of a malicious object |  | IPv6-address of a malicious object has been identified |  |  |
|  | Domain name of malicious object |  | Domain name of malicious object has been identified | List of domain names or file |  |
|  | URI-address of malicious object |  | URI-address of malicious object has been identified | List of URI-addresses or file |  |
|  | e-mail-address of malicious object or subject |  | E-mail-address of malicious object or subject has been identified | List of e-mail addresses or file |  |
|  | Malware file | CO | One of the fields must be filled in | File | To be filled in for at least one malware sample. |
|  |  |  |  |  | The block is to be filled in separately for each malware sample |
|  | URL for downloading |  |  | Text field |  |
|  | Hash sum | N | - | Text field |  |
|  | Hashing algorithm |  | - | [SHA256] [SHA1]  [MD5] |  |
|  | Number of identified attempts of malware deployment for the period of data aggregation | O | - | Number | - |
| Unsuccessful authorisation attempts | IPv4-address of malicious object | CO | IPv4-address of malicious object has been identified | List of IP-addresses or file | At least one of the fields is to be filled in  All the identified sources of malicious activity in the period of data aggregation are specified |
|  | IPv6-address of a malicious object |  | IPv6-address of a malicious object has been identified |  |  |
|  | Domain name of malicious object |  | Domain name of malicious object has been identified | List of domain names or file |  |
|  | URI-address of malicious object |  | Domain name of malicious object has been identified | List of domain names or file |  |
|  | Number of unique (for the combination source of malicious activity + account) unsuccessful attempts of authorisation for the period of data aggregation | O | - | Number | - |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name of computer attack** | **Information about malicious activity objects or subjects** | | | | |
| **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| Identification of phishing mailout or resource | IPv4-address of malicious object | CO | IPv4-address of malicious object has been identified | List of IP-addresses or file | At least one of the fields is to be filled in  All the identified sources of malicious activity in the period of data aggregation are specified |
|  | IPv6-address of a malicious object |  | IPv6-address of a malicious object has been identified |  |  |
|  | Domain name of malicious object |  | Domain name of malicious object has been identified | List of domain names or file |  |
|  | URI-address of malicious object |  | URI-address of malicious object has been identified | List of URI-addresses or file |  |
|  | e-mail-address of malicious object or subject |  | E-mail-address of malicious object or subject has been identified | List of e-mail addresses or file |  |
|  | Additional information about a technique of attack realisation | N | - | Text field | - |
| Attempts of social engineering | IPv4-address of malicious object | CO | IPv4-address of malicious object has been identified | List of IP-addresses or file | At least one of the fields is to be filled in  All the identified sources of malicious activity in the period of data aggregation are specified |
|  | IPv6-address of a malicious object |  | IPv6-address of a malicious object has been identified |  |  |
|  | Domain name of malicious object |  | Domain name of malicious object has been identified | List of domain names or file |  |
|  | URI-address of malicious object |  | URI-address of malicious object has been identified | List of URI-addresses or file |  |
|  | e-mail-address of malicious object or subject |  | E-mail-address of malicious object has been identified | List of e-mail addresses or file |  |
|  | Mobile telephone number of malicious subject |  | Mobile telephone number of malicious subject has been identified | List of mobile telephone numbers or file |  |
|  | Additional information about a technique of attack realisation  using social  engineering | N | - | Text field | - |
| Network scanning of controlled resource | IPv4-address of malicious object | CO | IPv4-address of malicious object has been identified | List of IP-addresses or file | At least one of the fields is to be filled in  All the identified sources of malicious activity in the period of data aggregation are specified |
|  | IPv6-address of a malicious object |  | IPv6-address of a malicious object has been identified |  |  |
|  | Domain name of malicious object |  | Domain name of malicious object has been identified | List of domain names or file |  |
|  | URI-address of malicious object |  | URI-address of malicious object has been identified | List of URI-addresses or file |  |
|  | Number of unique (for the combination source of scanning + scanned system) scanning events for the period of data aggregation | O | - | Number | - |

APPENDIX 22. DATA PROVISION FORMS NTF\_CA, PRE-FILLED FOR COMPUTER ATTACKS

|  |  |
| --- | --- |
| **Code of computer attack** | **Name of computer attack** |
| **[**[DoS](#_bookmark55)**]** | **"DoS (denial of service) attack"** |
| **[**[Exploit attempt](#_bookmark56)**]** | **Attempted use of vulnerability** |
| **[**[Infection attempt](#_bookmark57)**]** | **Attempted deployment of malware modules** |
| **[**[Login attempt](#_bookmark58)**]** | **Unsuccessful authorisation attempts** |
| **[**[Phishing](#_bookmark59)**]** | **Identification of phishing mailout or resource** |
| **[**[Social engineering](#_bookmark60)**]** | **Attempts of social engineering** |
| **[**[Scanning](#_bookmark61)**]** | **Network scanning of controlled resource** |

### Data provision form NTF\_CA\_DoS - Form of provision of data about computer attacks related to "Denial of service" computer attacks

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 1 | Type of notification | Type of notification | O | - | [NTF\_CA\_DoS] | Pre-filled field |
| 2 | Description of computer attack | Description of computer attack | N | - | Text field | Textual description of computer attack (including additional information  about CA realisation method, CA identification method etc.). Where a computer attack is identified  using information from the bulletin of the Bank of Russia or NCCCI, the number of such bulletin  is to be specified |
| 3 | Classification of computer attack | Vector of computer attack | O | - | [INT] | Pre-filled field |
| 4 | Type of computer attack | O | - | [DoS] | Pre-filled field |
| 5 | Date | Date as of which data about computer attacks are aggregated | O | - | In accordance with RFC 3339 | Moscow time [UTC +03:00] |
| 6 | Information about CII  facilities being the target of computer attacks | Name of controlled information resource | CO | To be filled in where attacks affecting a CII facility are identified | Text field | - |
| 7 | Category of controlled resource | [No relevance category]  [Third relevance category] [Second relevance category] [First relevance  category] | - |
| 8 | Country/region | In ISP-3166-2 format | - |
| 9 | IPv6-address of attacked resource | List of IP-addresses or file | One of the fields must be filled in |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 10 |  | IPv6-address of attacked resource |  |  |  |  |
| 11 | Domain name of attacked resource | List of domain names or file |
| 12 | URI-address of attacked resource | List of URI-addresses or file |
| 13 | e-mail address of attacked object | List of e-mail addresses or file |
| 14 | Attacked network service and port/protocol | Text field | To be filled in where information is available |
| 15 | Information about malicious activity objects or subjects | IPv4-address of malicious object | CO | IPv4-address of malicious object has been identified | List of IP-addresses or file | At least one of the fields is to be filled in  All the identified sources of malicious activity in the period of data aggregation are specified |
| 16 | IPv6-address of a malicious object | IPv6-address of a malicious object has been identified |
| 17 | Domain name of malicious object | Domain name of malicious object has been identified | List of domain names or file |
| 18 | Number of unique "denial of service" attacks (for the combination source of attack + attacked system) for the period of data aggregation | O | - | Number | - |
| 19 | Restrictive TLP marker | Restrictive marker for distribution of information from the given notification | N | - | [TLP: WHITE] [TLP: GREEN] [TLP: AMBER] [TLP: RED] | In accordance with designations accepted in TLP protocol.  Default value [TLP: GREEN], unless otherwise specified |

**Data provision form NTF\_CA\_Exploit attempt - Form of provision of data about computer attacks related to attempted use of vulnerabilities**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 1 | Type of notification | Type of notification | O | - | [NTF\_CA\_Exploit attempt] | Pre-filled field |
| 2 | Description of computer attack | Description of computer attack | N | - | Text field | Textual description of computer attack (including additional information  about CA realisation method, CA identification method etc.). Where a computer attack is identified  using information from the bulletin of the Bank of Russia or NCCCI, the number of such bulletin  is to be specified. |
| 3 | Classification of computer attack | Vector of computer attack | O | - | [INT] | Pre-filled field |
| 4 | Type of computer attack | O | - | [Exploit attempt] | Pre-filled field |
| 5 | Date | Date as of which data about computer attacks are aggregated | O | - | In accordance with RFC 3339 | Moscow time [UTC +03:00] |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 6 | Information about CII  facilities being the target of computer attacks | Name of controlled information resource | CO | To be filled in where attacks affecting a CII facility are identified | Text field | - |
| 7 | Category of controlled resource | [No relevance category]  [Third relevance category] [Second relevance category] [First relevance  category] | - |
| 8 | Country/region | In ISP-3166-2 format | - |
| 9 | IPv6-address of attacked resource | List of IP-addresses or file | One of the fields must be filled in |
| 10 | IPv6-address of attacked resource |  |
| 11 | Domain name of attacked resource | List of domain names or file |
| 12 | URI-address of attacked resource | List of URI-addresses or file |
| 13 | e-mail address of attacked object | List of e-mail addresses or file |
| 14 | Attacked network service and port/protocol | Text field | To be filled in where information is available |
| 15 | Information about malicious activity objects or subjects | IPv4-address of malicious object | CO | IPv4-address of malicious object has been identified | List of IP-addresses or file | At least one of the fields is to be filled in  All the identified sources of malicious activity in the period of data aggregation are specified |
| 16 |  | IPv6-address of a malicious object |  | IPv6-address of a malicious object has been identified |  |  |
| 17 |  | Domain name of malicious object |  | Domain name of malicious object has been identified | List of domain names or file |  |
| 18 |  | URI-address of malicious object |  | URI-address of malicious object has been identified | List of URI-addresses or file |  |
| 19 |  | e-mail-address of malicious object or subject |  | E-mail-address of malicious object or subject has been identified | List of e-mail addresses or file |  |
| 20 |  | List of vulnerabilities being the subject of their attempted use | CO | In case the identified vulnerability is described in any system of description of vulnerabilities | List of used vulnerabilities of security of software or hardware, from the respective catalogue (for instance, CVE, TDB FSTEC etc.) | One of blocks must be filled in |
| 21 |  | Name of system of description of vulnerabilities |  |  | Text field |  |
| 22 |  | Description of vulnerabilities | CO | In case the identified vulnerability is not described in any system of description of vulnerabilities | Text field |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 23 |  | Number of unique attempts of use (for the combination source of attack + attacked system) for the period of data aggregation | O | - | Number | - |
| 24 | Restrictive TLP marker | Restrictive marker for distribution of information from the given notification | N | - | [TLP: WHITE] [TLP: GREEN] [TLP: AMBER] [TLP: RED] | In accordance with designations accepted in TLP protocol.  Default value [TLP: GREEN], unless otherwise specified |

**Data provision form NTF\_CA\_Infection attempt - Form of provision of data about computer attacks related to attempted deployment of malware modules**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 1 | Type of notification | Type of notification | O | - | [NTF\_CA\_Infection attempt] | Pre-filled field |
| 2 | Description of computer attack | Description of computer attack | N | - | Text field | Textual description of computer attack (including additional information  about CA realisation method, CA identification method etc.). Where a computer attack is identified  using information from the bulletin of the Bank of Russia or NCCCI, the number of such bulletin  is to be specified |
| 3 | Classification of computer attack | Vector of computer attack | O | - | [EXT]  [INT] | [EXT] - targeted  at the client or counterparty of the financial institution ot other persons  cooperating with the financial institution  [INT] - targeted at computer objects  of financial institution |
| 4 | Type of computer attack | O | - | [Infection attempt] | Pre-filled field |
| 5 | Date | Date as of which data about computer attacks are aggregated | O | - | In accordance with RFC 3339 | Moscow time [UTC +03:00] |
| 6 | Information about CII  facilities being the target of computer attacks | Name of controlled information resource | CO | To be filled in where attacks affecting a CII facility are identified | Text field | - |
| 7 | Category of controlled resource | [No relevance category]  [Third relevance category] [Second relevance category] [First relevance  category] | - |
| 8 | Country/region | In ISP-3166-2 format | - |
| 9 | IPv6-address of attacked resource | List of IP-addresses or file | One of the fields must be filled in |
| 10 | IPv6-address of attacked resource |
| 11 | Domain name of attacked resource | List of domain names or file |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 12 |  | URI-address of attacked resource |  |  | List of URI-addresses or file | To be filled in where information is available |
| 13 | e-mail address of attacked object | List of e-mail addresses or file |
| 14 | Attacked network service and port/protocol | Text field |
| 15 | Information about malicious activity objects or subjects | IPv4-address of malicious object | CO | IPv4-address of malicious object has been identified | List of IP-addresses or file | All the identified sources of malicious activity in the period of data aggregation are specified |
| 16 | IPv6-address of a malicious object | IPv6-address of a malicious object has been identified |
| 17 | Domain name of malicious object | Domain name of malicious object has been identified | List of domain names or file |
| 18 | URI-address of malicious object | URI-address of malicious object has been identified | List of URI-addresses or file |
| 19 | e-mail-address of malicious object or subject | E-mail-address of malicious object or subject has been identified | List of e-mail addresses or file |
| 20 | Malware file | CO | One of the fields must be filled in | File | To be filled in for at least one malware sample.  The block is to be filled in separately for each malware sample |
| 21 | URL for downloading | Text field |
| 22 | Hash sum | N | - | Text field |
| 23 | Hashing algorithm |  | - | [SHA256] [SHA1]  [MD5] |
| 24 | Number of identified attempts of malware deployment for the period of data aggregation | O | - | Number | - |
| 25 | Restrictive TLP marker | Restrictive marker for distribution of information from the given notification | N | - | [TLP: WHITE] [TLP: GREEN] [TLP: AMBER] [TLP: RED] | In accordance with designations accepted in TLP protocol.  Default value [TLP: GREEN], unless otherwise specified |

**Data provision form NTF\_CA\_Login attempt - Form of provision of data about computer attacks related to unsuccessful authorisation attempts**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 1 | Type of notification | Type of notification | O | - | [NTF\_CA\_Login attempt] | Pre-filled field |
| 2 | Description of computer attack | Description of computer attack | N | - | Text field | Textual description of computer attack (including additional information  about CA realisation method, CA identification method etc.). Where a computer attack is identified  using information from the bulletin of the Bank of Russia or NCCCI, the number of such bulletin  is to be specified |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 3 | Classification of computer attack | Vector of computer attack | O | - | [EXT]  [INT] | [EXT] - targeted  at the client or counterparty of the financial institution ot other persons  cooperating with the financial institution  [INT] - targeted at computer objects  of financial institution |
| 4 | Type of computer attack | O | - | [Login attempt] | Pre-filled field |
| 5 | Date | Date as of which data about computer attacks are aggregated | O | - | In accordance with RFC 3339 | Moscow time [UTC +03:00] |
| 6 | Information about CII  facilities being the target of computer attacks | Name of controlled information resource | CO | To be filled in where attacks affecting a CII facility are identified | Text field | - |
| 7 | Category of controlled resource | [No relevance category]  [Third relevance category] [Second relevance category] [First relevance  category] | - |
| 8 | Country/region | In ISP-3166-2 format | - |
| 9 | IPv6-address of attacked resource | List of IP-addresses or file | One of the fields must be filled in |
| 10 | IPv6-address of attacked resource |  |
| 11 | Domain name of attacked resource | List of domain names or file |
| 12 | URI-address of attacked resource | List of URI-addresses or file |
| 13 | e-mail address of attacked object | List of e-mail addresses or file |
| 14 | Attacked network service and port/protocol | Text field | To be filled in where information is available |
| 15 | Information about malicious activity objects or subjects | IPv4-address of malicious object | CO | IPv4-address of malicious object has been identified | List of IP-addresses or file | At least one of the fields is to be filled in  All the identified sources of malicious activity in the period of data aggregation are specified |
| 16 |  | IPv6-address of a malicious object |  | IPv6-address of a malicious object has been identified |  |  |
| 17 |  | Domain name of malicious object |  | Domain name of malicious object has been identified | List of domain names or file |  |
| 18 |  | URI-address of malicious object |  | Domain name of malicious object has been identified | List of domain names or file |  |
| 19 |  | Number of unique (for the combination source of malicious activity + account) unsuccessful attempts of authorisation for the period of data aggregation | O | - | Number | - |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 20 | Restrictive TLP marker | Restrictive marker for distribution of information from the given notification | N | - | [TLP: WHITE] [TLP: GREEN] [TLP: AMBER] [TLP: RED] | In accordance with designations accepted in TLP protocol.  Default value [TLP: GREEN], unless otherwise specified |

**Data provision form NTF\_CA\_Phishing - Form of provision of data about computer attacks related to phishing mailouts or resources**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 1 | Type of notification | Type of notification | O | - | [NTF\_CA\_Phishing] | Pre-filled field |
| 2 | Description of computer attack | Description of computer attack | N | - | Text field | Textual description of computer attack (including additional information  about CA realisation method, CA identification method etc.). Where a computer attack is identified  using information from the bulletin of the Bank of Russia or NCCCI, the number of such bulletin  is to be specified |
| 3 | Classification of computer attack | Vector of computer attack | O | - | [EXT]  [INT] | [EXT] - targeted  at the client or counterparty of the financial institution ot other persons  cooperating with the financial institution  [INT] - targeted at computer objects  of financial institution |
| 4 | Type of computer attack | O | - | [Phishing] | Pre-filled field |
| 5 | Date | Date as of which data about computer attacks are aggregated | O | - | In accordance with RFC 3339 | Moscow time [UTC +03:00] |
| 6 | Information about CII  facilities being the target of computer attacks | Name of controlled information resource | CO | To be filled in where attacks affecting a CII facility are identified | Text field | - |
| 7 | Category of controlled resource | [No relevance category]  [Third relevance category] [Second relevance category] [First relevance  category] | - |
| 8 | Country/region | In ISP-3166-2 format | - |
| 9 | IPv6-address of attacked resource | List of IP-addresses or file | One of the fields must be filled in |
| 10 | IPv6-address of attacked resource |
| 11 | Domain name of attacked resource | List of domain names or file |
| 12 | URI-address of attacked resource | List of URI-addresses or file |
| 13 | e-mail address of attacked object | List of e-mail addresses or file |
| 14 | Attacked network service and port/protocol | Text field | To be filled in where information is available |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 15 | Information about malicious activity objects or subjects | IPv4-address of malicious object | CO | IPv4-address of malicious object has been identified | List of IP-addresses or file | At least one of the fields is to be filled in  All the identified sources of malicious activity in the period of data aggregation are specified |
| 16 | IPv6-address of a malicious object | IPv6-address of a malicious object has been identified |
| 17 | Domain name of malicious object | Domain name of malicious object has been identified | List of domain names or file |
| 18 | URI-address of malicious object | URI-address of malicious object has been identified | List of URI-addresses or file |
| 19 | e-mail-address of malicious object or subject | E-mail-address of malicious object or subject has been identified | List of e-mail addresses or file |
| 20 | Additional information about a technique of attack realisation | N | - | Text field | - |
| 21 | Restrictive TLP marker | Restrictive marker for distribution of information from the given notification | N | - | "[TLP: WHITE] [TLP: GREEN] [TLP: AMBER] [TLP: RED] " | In accordance with designations accepted in TLP protocol.  Default value [TLP: GREEN], unless otherwise specified |

**Data provision form NTF\_CA\_Social engineering - Form of provision of data about computer attacks related to attempts of social engineering.**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 1 | Type of notification | Type of notification | O | - | [NTF\_CA\_Social engineering] | Pre-filled field |
| 2 | Description of computer attack | Description of computer attack | N | - | Text field | Textual description of computer attack (including additional information  about CA realisation method, CA identification method etc.). Where a computer attack is identified  using information from the bulletin of the Bank of Russia or NCCCI, the number of such bulletin  is to be specified |
| 3 | Classification of computer attack | Vector of computer attack | O | - | [EXT]  [INT] | [EXT] - targeted  at the client or counterparty of the financial institution ot other persons  cooperating with the financial institution  [INT] - targeted at computer objects  of financial institution |
| 4 | Type of computer attack | O | - | [Social engineering] | Pre-filled field |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 5 | Date | Date as of which data about computer attacks are aggregated | O | - | In accordance with RFC 3339 | Moscow time [UTC +03:00] |
| 6 | Information about CII  facilities being the target of computer attacks | Name of controlled information resource | CO | To be filled in where attacks affecting a CII facility are identified | Text field | - |
| 7 | Category of controlled resource | [No relevance category]  [Third relevance category] [Second relevance category] [First relevance  category] | - |
| 8 | Country/region | In ISP-3166-2 format | - |
| 9 | IPv6-address of attacked resource | List of IP-addresses or file | One of the fields must be filled in |
| 10 | IPv6-address of attacked resource |
| 11 | Domain name of attacked resource | List of domain names or file |
| 12 | URI-address of attacked resource | List of URI-addresses or file |
| 13 | e-mail address of attacked object | List of e-mail addresses or file |
| 14 | Attacked network service and port/protocol | Text field | To be filled in where information is available |
| 15 | Information about malicious activity objects or subjects | IPv4-address of malicious object | CO | IPv4-address of malicious object has been identified | List of IP-addresses or file | At least one of the fields is to be filled in  All the identified sources of malicious activity in the period of data aggregation are specified |
| 16 |  | IPv6-address of a malicious object |  | IPv6-address of a malicious object has been identified |  |  |
| 17 |  | Domain name of malicious object |  | Domain name of malicious object has been identified | List of domain names or file |  |
| 18 |  | URI-address of malicious object |  | URI-address of malicious object has been identified | List of URI-addresses or file |  |
| 19 |  | e-mail-address of malicious object or subject |  | E-mail-address of malicious object has been identified | List of e-mail addresses or file |  |
| 20 |  | Mobile telephone number of malicious subject |  | Mobile telephone number of malicious subject has been identified | List of mobile telephone numbers or file |  |
| 21 |  | Additional information about a technique of attack realisation using social engineering | N | - | Text field | - |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 22 | Restrictive TLP marker | Restrictive marker for distribution of information from the given notification | N | - | [TLP: WHITE] [TLP: GREEN] [TLP: AMBER] [TLP: RED] | In accordance with designations accepted in TLP protocol.  Default value [TLP: GREEN], unless otherwise specified |

**Data provision form NTF\_CA\_Scanning - Form of provision of data about computer attacks related to network scanning of a controlled resource**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Sequential number | Category of data element | Description of AIPS UI | Field applicability | Condition of applicability | Fill-in rule | Note |
| 1 | Type of notification | Type of notification | O | - | [NTF\_CA\_Scanning] | Pre-filled field |
| 2 | Description of computer attack | Description of computer attack | N | - | Text field | Textual description of computer attack (including additional information  about CA realisation method, CA identification method etc.). Where a computer attack is identified  using information from the bulletin of the Bank of Russia or NCCCI, the number of such bulletin  is to be specified |
| 3 | Classification of computer attack | Vector of computer attack | O | - | [INT] | Pre-filled field |
| 4 | Type of computer attack | O | - | [Scanning] | Pre-filled field |
| 5 | Date | Date as of which data about computer attacks are aggregated | O | - | In accordance with RFC 3339 | Moscow time [UTC +03:00] |
| 6 | Information about CII  facilities being the target of computer attacks | Name of controlled information resource | CO | To be filled in where attacks affecting a CII facility are identified | Text field | - |
| 7 | Category of controlled resource | [No relevance category]  [Third relevance category] [Second relevance category] [First relevance  category] | - |
| 8 | Country/region | In ISP-3166-2 format | - |
| 9 | IPv6-address of attacked resource | List of IP-addresses or file | One of the fields must be filled in |
| 10 | IPv6-address of attacked resource |
| 11 | Domain name of attacked resource | List of domain names or file |
| 12 | URI-address of attacked resource | List of URI-addresses or file |
| 13 | e-mail address of attacked object | List of e-mail addresses or file |
| 14 | Attacked network service and port/protocol | Text field | To be filled in where information is available |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 15 | Information about malicious activity objects or subjects | IPv4-address of malicious object | CO | IPv4-address of malicious object has been identified | List of IP-addresses or file | At least one of the fields is to be filled in  All the identified sources of malicious activity in the period of data aggregation are specified |
| 16 | IPv6-address of a malicious object | IPv6-address of a malicious object has been identified |
| 17 | Domain name of malicious object | Domain name of malicious object has been identified | List of domain names or file |
| 18 | URI-address of malicious object | URI-address of malicious object has been identified | List of URI-addresses or file |
| 19 | Number of unique (for the combination source of scanning + scanned system) scanning events for the period of data aggregation | O | - | Number | - |
| 20 | Restrictive TLP marker | Restrictive marker for distribution of information from the given notification | N | - | [TLP: WHITE] [TLP: GREEN] [TLP: AMBER] [TLP: RED] | In accordance with designations accepted in TLP protocol.  Default value [TLP: GREEN], unless otherwise specified |

APPENDIX 23. DATA PROVISION FORM NTF\_VULNERABILITIES –

FORM OF PROVISION BY INFORMATION EXCHANGE PARTICIPANTS OF DATA ABOUT IDENTIFIED INFORMATION SECURITY VULNERABILITIES

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 1 | Type of notification | | Type of notification | O | - | [NTF\_Vulnerabilities] | Pre-filled field |
| 2 | General information about conducted vulnerability analysis | | Date of vulnerability analysis | O | - | In accordance with RFC 3339 | Moscow time [UTC +03:00] |
| 3 | Entity having conducted vulnerability analysis | O | - | Name of the entity having conducted vulnerability analysis or [Unaided analysis] | - |
| 4 | Results of conducted vulnerability analysis (to be filled in separately for each computer object in which a vulnerability has been identified) | Description of computer object, in which a vulnerability has been identified | Level of computer object in which a vulnerability has been identified | O | - | From the classifier  "Types of objects and subjects" set forth  in [Appendix 28](#_bookmark67) | - |
| 5 | Type of computer object, in which a vulnerability has been identified | O | - | From the classifier  "Types of objects and subjects" set forth in [Appendix 28](#_bookmark67) | The list depends  on the field "Level of computer object in which a vulnerability has been  identified" |
| 6 | Computer object, in which a vulnerability has been identified in CPE format | O | - | In the format consistent with the recommendations of the Bank of Russia published on the official website | - |
| 7 | Category of controlled resource | CO | If it is a CII object | [No relevance category]  [Third relevance category] [Second relevance category] [First relevance  category] | - |
| 8 | Availability of Internet connection | O | - | [Yes]/[No] | - |
| 9 | Technical information about computer object  in which a vulnerability has been identified | IPv4-address (routable) of computer object | CO | The fields identifying a specific computer object are to be filled in | Text field | At least one of the elements must be filled in |
| 10 | IPv6-address (routable) of computer object | Text field |
| 11 | Domain name associated with the computer object | Text field |
| 12 | URI-address of computer object | Text field |
| 13 | Number of attacked autonomous system (ASN) | Text field |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 14 |  | Description of identified vulnerabilities (to be filled in separately for each vulnerability identified in the computer  object) | Vulnerability of computer object | CO | Where the identified vulnerability is described  in the system of description of vulnerabilities | Text field  Where several security vulnerabilities are used, they are specified using "+" | One of blocks must be filled in |
| 15 | Name of system of description of vulnerabilities | [CVE]  [TDB FSTEC] |
| 16 | Description of vulnerability | CO | In case the identified vulnerability is not described in any system of description of vulnerabilities | Text field |
| 17 | Measures taken to respond to identified vulnerabilities | Status of rectification of identified weaknesses and vulnerabilities of computer object | O | - | [Fixed] [inProcess] | [Fixed] - measures have been taken, the vulnerability has been rectified [inProcess] - measures to rectify the vulnerability are being taken |
| 18 |  | Measures taken to respond to vulnerability | CO | "Status of rectification of identified weaknesses and vulnerabilities of computer object" = [Fixed] | Text field | Detailed description of measures taken to respond to vulnerability |

APPENDIX 24. DATA PROVISION FORM REQ\_IEP\_DETECT - FORM OF THE BANK OF RUSSIA'S REQUEST FOR THE PURPOSES OF RECEIVING INFORMATION OF AN IDENTIFIED

COMPUTER ATTACK OR AN INFORMATION SECURITY VULNERABILITY

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 1 | Type of request/response | Type of request/response | O | - | [REQ\_IEP\_Detect] | Pre-filled field |
| 2 | Type of event | Type of identified event | O | - | [Infected resource] [Source of e-mail distribution of malware modules] [Source of distribution of malware modules] [Malware management center] [Malware infrastructure element]  [Slowed down operation of a resource]  [Source of vulnerability use]  [Source of account compromise] [Participant of network capture of traffic] [Source of unauthorised access] [Source of unauthorised modification of information]  [Source of spam distribution] [Publication of information prohibited by the legislation of the Russian Federation] [Placement of phishing resource]  [Existence of unauthorised content] [DDoS-attack participant] [Compromised account] [Source of network scanning] [Participant of fraud] [Source of social engineering threat] [Vulnerable resource] [Suspected phishing resource]  [Threat of PD compromise]  [Threat of computer  attack] | - |
| 3 | Description of information security event | Description of identified information security event | N | - | Text field | Textual description of identified information security event |
| 4 | Date and time of information  security event | Date and time of identification of information security event | O | - | In accordance with RFC 3339 | Moscow time [UTC +03:00] |
| 5 | Date and time of completion of information security event | CO | In case of availability of | In accordance with RFC 3339 | Moscow time [UTC +03:00] |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 6 | Information resource owner | Information resource owner | O | - | Text field | - |
| 7 | Information about objects being the target of the information security event | IPv6-address of attacked resource | CO | In case of availability of respective information | List of IP-addresses | - |
| 8 | IPv6-address of attacked resource |
| 9 | Domain name of attacked resource | List of domain names |
|  | Name of domain registrar | List of names of domain registrars |
| 10 | URI-address of attacked resource | List of URI-addresses |
| 11 | e-mail address of attacked object | List of e-mail addresses |
| 12 | Attacked network service and port/protocol | Text field | - |
| 13 | AS-Path to the attacked autonomous system (ASN) | Text field |
| 14 | Information about malicious  activity objects having caused the information security event | IPv4-address of malicious object | CO | IPv4-address of malicious object has been identified | List of IP-addresses | - |
| 15 | IPv6-address of a malicious object | IPv6-address of a malicious object has been identified | - |
| 16 | Domain name of malicious object | Domain name of malicious object has been identified | List of domain names | - |
|  | Name of domain registrar | List of names of domain registrars |  |
| 17 | URI-address of malicious object | URI-address of malicious object has been identified | List of URI-addresses | - |
| 18 | e-mail-address of malicious object or subject | E-mail-address of malicious object or subject has been identified | List of e-mail addresses | - |
| 19 | Malware file | CO | One of the fields must be filled in | File | - |
| 20 | URL for downloading | Text field | - |
| 21 | Hash sum | O | - | Text field | - |
| 22 | Hashing algorithm |  | - | [SHA256] [SHA1]  [MD5] | - |
| 23 | Vulnerability | CO | Where the fact of use of vulnerabilities by malware has been identified | List of used vulnerabilities of security of software or hardware, from the respective catalogue (for instance, CVE, TDB FSTEC etc.) | - |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 24 |  | Name of system of description of vulnerabilities |  |  | Text field | - |
| 25 | Description of vulnerability not described in any system of description of vulnerabilities | Text field | - |
| 26 | Number of dummy autonomous system (ASN) | O | - | Text field | - |
| 27 | AS name | O | - | Text field | - |
| 28 | LIR name | O | - | Text field | - |
| 29 | Restrictive TLP marker | Restrictive marker for distribution of information from the given notification | N | - | [TLP: WHITE] [TLP: GREEN] [TLP: AMBER] [TLP: RED] | In accordance with designations accepted in TLP protocol.  Default value [TLP: GREEN], unless otherwise specified |

### Data provision form RESP\_IEP\_Detect - Form of submission of response to the Bank of Russia's request for the purposes of receiving information of an identified computer attack or an information security vulnerability

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 1 | Type of request/response | Type of request/response | O | - | [RESP\_IEP\_Detect] | Pre-filled field |
| 2 | Result of adopted decision | Result of adopted decision | O | - | [Measures have been taken] [Information has been recorded] [Information has not been acknowledged] | - |

APPENDIX 25. DATA PROVISION FORM REQ\_IEP\_ISWEBSITE - FORM OF REQUEST OF THE BANK OF RUSSIA FOR THE PURPOSES OF RECEIVING DATA ABOUT AN INFORMATION EXCHANGE PARTICIPANT'S OWNERSHIP OF AN INTERNET RESOURCE

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 1 | Type of request/response | Type of request/response | O | - | [INQ\_WEB\_REQ] | Pre-filled field |
| 2 | General information of the request | Description | O | - | Text field | - |
| 3 |  | Legal reasoning | O | - | Text field | - |
| 4 |  | URL-address of resource | CO | At least | Text field | - |
|  |  |  |  | one field |  |  |
|  |  |  |  | is to be filled in |  |  |
| 5 |  | IP-address of resource | CO |  | Text field | - |
| 6 |  | Domain name of attacked resource | CO |  | Text field | - |
| 7 |  | Distribution of | CO | Where distribution of | [Yes] | - |
|  |  | malware, |  | malware, |  |  |
|  |  | phishing information |  | phishing |  |  |
|  |  | or information prohibited |  | information |  |  |
|  |  | by the legislation of the Russian Federation is carried out |  | or information |  |  |
|  |  | prohibited |  | by the legislation  of the Russian Federation is carried out |  |  |

### Data provision form RESP\_IEP\_IsWebSite - Form of submission of response to the request of the Bank of Russia for the purposes of receiving data about an information exchange participant's ownership of an Internet resource

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 1 | Type of request/response | Type of request/response | O | - | [INQ\_WEB\_RESP] | Pre-filled field |
| 2 | General data of response to the request | Owned by the entity | O | - | [Yes]  [No] | - |
| 3 | URL-address of resource | CO | "Owned by the entity"  = [Yes] | Text field | The fields not filled out in the incoming request are to be filled in |
| 4 | IP-address of resource | CO | Text field |
| 5 | Domain name of attacked resource | CO | Text field |
| 6 | Description of measures to combat malware distribution | CO | "Owned by the entity"  = [Yes] | Text field | - |
| 7 | Is the specified resource, in the entity's opinion, distributing malware, phishing information or information prohibited by the legislation of the Russian Federation | CO | "Owned by the entity" = [No] | [Yes]  [No] | - |
| 8 | Consent to the Bank of Russia's taking of measures  to block  the given resource | CO | "Owned by the entity" = [No] | [Yes]  [No] | - |

APPENDIX 26. DATA PROVISION FORM REQ\_IEP\_CORRACCLOCK –

FORM OF PROVISION OF DATA USED FOR REQUESTS TO THE BANK OF RUSSIA BY INFORMATION EXCHANGE PARTICIPANTS USING AN EXPRESS AND NON-EXPRESS TRANSFER SERVICE TO TRANSFER

FUNDS, NOT BEING SUBDIVISIONS OF THE BANK OF RUSSIA,

ON IMPOSING (RELEASING) RESTRICTIONS IN RESPECT OF THEIR BANK (CORRESPONDENT) ACCOUNTS (SUBACCOUNTS) IN THE FORM OF A PROHIBITION TO DEBIT FUNDS UPON IDENTIFICATION OF INFORMATION SECURITY INCIDENTS DURING

FUNDS TRANSFERS USING

INFORMATION INFRASTRUCTURE FACILITIES OF INFORMATION EXCHANGE PARTICIPANTS

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 1 | Type of request/response | Type of request/response | O | - | [REQ\_IEP\_CorrAccLock] | Pre-filled field |
| 2 | System used | Type of system | O | - | Selection of one of the values:  [PSBR]  [SPFS] | [PSBR] - payment system of the Bank of Russia  [SPFS] - financial messaging system  of the Bank of Russia |
| 3 | Type of participant | Type of participant | O | "Type of system" = [SPFS] | Selection of one of the values:  [AGT] [STDALN\_MEMBER] [SERV\_BR] [CSTSERV\_BR] | [AGT] - agent. Legal entity - SPFS user having concluded an agreement with the Bank of Russia containing terms and conditions on provision by the Bank of Russia of financial messaging services and conditions of transfer of third-party financial information via SPFS (standalone users (clients of service-bureau) [STDALN\_MEMBER]/[SERV\_  BR] - standalone user of SPFS/Service-bureau. User of SPFS having established contractual relationship with user of SPFS entitled to  to transfer third-party financial information (agent).  [CSTSERV\_BR] - client of service-bureau - a legal entity having concluded with the service bureau an agreement for transfer of financial messages  via SPFS |
| 4 | General information | Information system participant | O | - | Text field | - |
| 5 | Registration number | O | "Type of system" = [PSBR] | Text field | - |
| 6 | Participant's BIC | O | "Type of system" = [PSBR] | Text field | - |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 7 |  | Operation | O | - | Selection of one of the values:  [ON]  [OFF] | [ON] - in case of imposing restrictions in respect of bank (correspondent) accounts (subaccounts) in the form of a prohibition to debit funds or suspension of exchange of electronic financial messages via SPFS  [OFF] - in case of releasing restrictions in respect of bank (correspondent) accounts (subaccounts) in the form of a prohibition to debit funds or releasing restrictions to exchange electronic financial messages via SPFS |
| 8 | Date of performance of operation | O | - | Date and time in the format: datedmm.yyyy hh: mm | [UTC +03:00] |
| 9 | Description | N | - | Text field | - |
| 10 | Enclosure | O | - | File | - |
| 11 | Contact person | Surname | O | - | Text field | - |
| 12 | Name | O | - | Text field | - |
| 13 | Patronymic | O | - | Text field | - |
| 14 | Title | O | - | Text field | - |
| 15 | e-mail address | O | - | Text field | - |
| 16 | Landline telephone number | O | - | Text field | - |
| 17 | Mobile telephone number | O | - | Text field | - |

### Data provision form RESP\_IEP\_CorrAccLock - Form of provision of data used by the Bank of Russia to inform of imposing (or releasing) restrictions in respect of bank (correspondent) accounts (subaccounts) of information exchange participants in the form of a prohibition to debit funds

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 1 | Type of request/response | Type of request/response | O | - | [RESP\_IEP\_CorrAccLock] | Pre-filled field |
| 2 | General information | Status of request | O | - | [Executed] [Dismissed] | - |
| 3 | Comments | N | - | Text field | - |

APPENDIX 27. DATA PROVISION FORM NTF\_IEP\_PUBLICATION – FORM OF PROVISION BY INFORMATION EXCHANGE PARTICIPANTS OF DATA

ON THE PLANNED MEASURES TO DISCLOSE INFORMATION ABOUT IDENTIFIED INFORMATION SECURITY AND OPERATIONAL RELIABILITY INCIDENTS

INCIDENTS

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Sequential number** | **Category of data element** | **Description of AIPS UI** | **Field applicability** | **Condition of applicability** | **Fill-in rule** | **Note** |
| 1 | Type of notification | Type of notification | O | - | [NTF\_IEP\_Publication] | Pre-filled field |
| 2 | General information | Name of measure | O | - | Text field | - |
| 3 | Date of measure | O | - | Date and time in the format: datedmm.yyyy hh: mm | [UTC +03:00] |
| 4 | Description | O | - | Text field | - |
| 5 | Entity | O | - | Text field | - |
| 6 | Contact person | Surname | O | - | Text field | - |
| 7 | Name | O | - | Text field | - |
| 8 | Patronymic | N | - | Text field | - |
| 9 | Title | O | - | Text field | - |
| 10 | e-mail address | O | - | In accordance with RFC 822 | - |
| 11 | Landline telephone number | O | - | In accordance with the international numbering system and plan | - |
| 12 | Mobile telephone number | O | - | In accordance with the international numbering system and plan | - |
| 13 | Measure | Type of measure | O | - | Text field | - |
| 14 | Measure text | O | - | Text field or file | - |

APPENDIX 28. ADDITIONAL CLASSIFIERS USED IN THIS STANDARD

|  |  |
| --- | --- |
| **Name of classifier** | **Description of classifier** |
| [Criteria of legitimacy of operation without consent](#_bookmark68) | Signs of funds transfer without consent of the client established by the Bank of Russia |
| [Risk sources](#_bookmark69) | Classifier of information security threat risk events broken down by risk sources in accordance with GOST R 57580.3-2022 |
| [Types of objects and subjects](#_bookmark70) | Classifier of risk sources broken down by areas of types of attacked objects in accordance with GOST R 57580.3-2022 |
| [Technological sites](#_bookmark71) | Classifier of technological sites in accordance with regulatory acts of the Bank of Russia |

CLASSIFIER "CRITERIA OF LEGITIMACY OF OPERATION WITHOUT CONSENT"

|  |  |  |
| --- | --- | --- |
| **Field of data provision form** | **Code of legitimacy criterion** | **Legitimacy criterion** |
| Criteria of legitimacy of operation without consent characterising the payer | [Statement] | Availability of payer's application about disagreement with the operation |
| [Atypical device] | Inconsistency of device used to perform the operation or device parameters typical for payer's operations |
| [Atypical actions] | Inconsistency of acts preceding the operation with typical acts (withdrawal of deposit, multiple receipts from various payers, change of telephone number, receiving OTP etc.) |
| [Atypical session] | Inconsistency of behavior during the session with typical behavior (the session is opened without completion of the previous session, request of several one time passwords, multiple unsuccessful OTP attempts etc.) |
| [Robotisation] | Identification of automated acts upon payment generation |
| [Absence] | Non-availability for the payer of other financial products (credit products, investment products etc.) |
| [Mass registration] | Mass registration / opening of payment instruments (cards, accounts) |
| [Spoof of payment] | Signs of details spoofing on part of the payer |
| [Questionable source] | Signs of receiving details of the payee from an unreliable source |
| [Remote control] | Signs of remote access to the payer's device |
| [SIM replacement] | Signs of replacement of the client's SIM-card |
| [Confirmed transactions] | Performance by the payer of previous operations to the given payee which have not been disputed |
| [Subscription] | Periodical payments (subscriptions) of the payer to the given payee which have not been disputed |
| [Virus] | Signs of impact of malicious software on the client's device |
| [Change login/password] | Repeated registration or resumption of access to RBS, change of login/password for access |
| [Tokenisation] | Binding, tokenisation of payment instruments (cards) to a non-typical device or to several devices |
| [Retiree] | Is an elderly person or pensioner |
| [Anonymous] | Signs of use by the payer of anonymised communications channels, public VPN and proxy, cloud and dedicated servers |
| [Mass Retail] | Existence of large number of purchase operations non-typical for the client |

|  |  |  |
| --- | --- | --- |
| **Field of data provision form** | **Code of legitimacy criterion** | **Legitimacy criterion** |
| Criteria of legitimacy of operation without consent characterising the funds recipient | [Statement] | Availability of applications about disagreement with the operation to the address of the given payee |
| [Geolocation] | Simultaneous work in RBS using different geolocations |
| [Excceeding device] | Using various devices to log into RBS, with the number of devices exceeding the average number |
| [Absence] | Non-availability for the payer of other financial products (credit products, investment products etc.) |
| [Mass registration] | Mass registration / opening of payment instruments (cards, accounts) |
| [Cashing out] | Cash out transactions in the absence of other operations |
| [Dropper] | Existence of a large number of operations to transfer funds (C2C, B2B) in the absence of other operations |
| [Relationship] | Identified relation (administrative, financial, technical etc.) to the persons included in the database on cases and attempts of funds transfers without consent of the client |
| [Absence transaction] | Absence of business activity operations in the client's profile |
| [Anonymous] | Signs of use by the recipient of anonymised communications channels, public VPN and proxy, cloud and dedicated servers |
| [Figurehead] | Signs of nominal management of the entity |
| [Titular owner] | Signs of nominal holder of a payment instrument (card, account) |
| [Complaints] | Existence of complaint to Internet fraud |
| [Fraud/Sale] | Exceedance of the ratio between fraud and non-fraud operations for the given recipient (in respect of the amount and number) over threshold values established by the credit institution |
| [Crypto] | Recipient's payment facility is used for cryptocurrency operations |
| [Confirmed transactions] | Previous receipt of funds from the given payer which has not been disputed |
| [Wage] | Existence of payroll card program |
| [Technological account] | The funds recipient's account is a technological account |
| [Subscription] | Periodical payments (subscriptions) to the given recipient which have not been disputed |
| [Government] | Is a public authority |
| [Financial institution] | Is an entity in the financial domain (credit institutions, subjects of the National payment system, non-banking financial institutions) |
| [GKH] | Is a payment agent in the sphere of housing and utilities |
| [Retail] | Is a large organisation engaged in retail sales |
| [Vendor] | Is a large organisation - supplier of goods or services |
| [Mediator] | Is an intermediate recipient of the operation (for instance P2P transfer service) |
| [Charity] | Is a charitable organisation |
| Criteria of legitimacy of operation without consent characterising the operation | [Atypical parametres] | Inconsistency of operation parameters with typical operations of the payer (amount of operation, regularity of operations, funds recipient etc.) |
| [Atypical conditions] | Inconsistency of conditions of operation with the conditions typical for the payer (payer's geolocation, time of the day of operations etc.) |
| [Atypical actions] | Inconsistency of acts preceding the operation with typical acts (withdrawal of deposit, multiple receipts from various payers, change of telephone number, receiving OTP etc.) |
| [Atypical device] | Inconsistency of device used to perform the operation or device parameters typical for payer's operations |
| [Mass Retail] | Large number of purchase operations for a short period of time non-typical for the client |
| [Credit after new auth] | Execution of pre-approved credit product right after resumption of access to RBS, change of login/password, OTP telephone number |
| [Dispute] | The operation is disputed as part of IPS complaint cycle or non-received goods/service |

CLASSIFIER "RISK SOURCES"

|  |  |  |
| --- | --- | --- |
| **Code of risk source** | **Name of risk source** | **Additional classification of information security threat risk events** |
| [defectOfProcess] | Defects of processes | For the purposes of additional classification of information security threat risk events the financial institution shall refer to the category "defects of processes":  defects of processes of applying technological measures to protect information processed as part of technological operations upon performance of business and technological processes;  defects of processes of using applied software of automated systems and applications consistent with information security requirements [8 - 10];  defects of processes of planning, realising, controlling and improving processes ensuring operational reliability and information security;  defects of other internal processes related to ensuring operational  reliability and information security of a financial institution |
| [actionOfStaff] | Acts of personnel and other persons related to a financial institution | For the purposes of additional classification of information security threat risk events the financial institution shall refer to the category "acts of personnel and other persons related to a financial institution" realisation of unauthorised access of employees of the financial institution or third parties having access  rights in respect of computer objects at infrastructure level of the financial institution  (acts of internal wrongdoer) |
| [failureOfIT] | Failures of computer objects (breakdown and (or) malfunction  of computer objects applied by the financial institution and (or) inconsistency of their functionalities and characteristics with the needs of the financial  institution) | For the purposes of additional classification of information security threat risk events the financial institution shall refer to the category "failures of computer objects" failures and breakdown of computer objects as a result of information threat materialisation |
| [externalFactor] | External factors | For the purposes of additional classification of information security threat risk events the financial institution shall refer to the category "external factors" any realised computer attacks or unauthorised access of persons not having access rights in respect of computer objects at infrastructure level of the financial institution (acts of external wrongdoer), in particular, to:  block standard operation of business and technological processes of the financial institution;  steal, distort, delete confidential information (including  personal data) |

CLASSIFIER "TYPES OF OBJECTS AND SUBJECTS"

|  |  |  |  |
| --- | --- | --- | --- |
| **Code of level of object or subject** | **Level of object or subject** | **Code of type of object or subject** | **Type of object or subject** |
| [Infrastructure] | Infrastructure level of computer objects (system level of information infrastructure) | [Hardware] | Hardware |
| [Network hardware] | Network equipment |
| [Network applications and services] | Network applications and services |
| [Server virtualisation components, software infrastructure services] | Server virtualisation components, software infrastructure services |
| [Operating systems, database management systems, application servers] | Operating systems, database management systems, application servers |
| [Application level to perform tech processes] | Application level of computer objects (level of automated systems and  applications) used to perform business and technological processes of the financial institution upon provision of financial (banking) and (or) information services | [System of remote banking] | Remote banking services systems |
| [System for processing transactions made using payment cards] | System for processing transactions made using payment cards] |
| [Information resource of the Internet] | Information resource of the Internet |
| [Automated banking system] | Automated banking system |
| [Post-transaction service system made using payment cards] | Post-transaction service system for operations made using payment cards |
| [Automated systems] | Automated systems used by employees of the financial institution |
| [Application level used by the client] | Application level of computer objects (level of automated systems and applications) used by the client of the financial institution upon receipt of financial services | [Mobile application] | Mobile application |
| [File server] | File server |
| [System of remote banking] | Remote banking services systems |
| [Email server] | E-mail server |
| [Automated system] | Automated system used by employees of the client of the financial institution |
| [Other object] | Other attacked objects | [Other system] | Other systems used by the financial institution |
| [Subject] | Attacked subjects | [Employee] | Employees of the financial institution |
| [Client] | Clients of the financial institution |
| [Partner] | Partners, counterparties, contractors etc. of the financial institution |

CLASSIFIER "TECHNOLOGICAL SITES"

|  |  |
| --- | --- |
| Code of technological site | Name of technological site |
| [IAA] | Identification, authentication and authorisation of clients upon performance of acts to carry out banking operations/financial operations or processing, storage and transfer of protected information |
| [FTA] | Formation (preparation), transfer and acceptance of e-messages |
| [AR] | Authorisation of clients' right to dispose of funds, securities or other property or to perform acts with protected information |
| [PR] | Performance of a banking operation/financial operation or acts for the purposes of processing, storage and transfer of protected information, recording of their results |
| [SI] | Storage/recording of e-messages, information about performance of banking/financial operations or acts with protected information, results of acts for the purposes of processing, storage and transfer of protected information |
| [ColB\_UBS]  [ColB\_CBS] | For UBS: collection of biometric personal data of natural persons and transfer of collected biometric personal data of natural persons between structural subdivisions of the bank, mobile (portable) computer devices (tablets), payment terminals, ATM.  For CBS: collection of biometric personal data of natural persons by financial institutions for the purposes of transfer to information systems of financial market institutions and transfer of collected biometric personal data of natural persons between structural subdivisions of the bank, mobile (portable) computer devices (tablets), payment terminals, ATM |
| [ProcessingB\_UBS]  [ProcessingB\_CBS] | For UBS: processing of collected biometric personal data of natural persons for the purpose of transfer to UBS using IEIS (Interdepartmental electronic interaction system).  For CBS: processing of biometric personal data of natural persons by financial institutions for their placement (updating) in information systems of financial market institutions |
| [TransferB\_UBS] | For UBS: transfer of biometric personal data of natural persons to UBS using IEIS |
| [RIA\_UBS]  [RIA\_CBS] | For UBS: remote identification or remote authentication of the client - natural person.  For CBS: automated transfer of biometric personal data of natural persons to information systems of financial market institutions and their processing on the client's - natural person's device to identify the natural person without its personal presence using biometric personal data (hereinafter, remote identification) and (or) authentication of natural person without its personal presence using biometric personal data (hereinafter, remote authentication) of the natural person |
| [CheckRIA\_UBS] | For UBS: checking the results of remote identification or remote authentication of the client - natural person in USIA (Unified system of identification and authentication) and UBS |
| [InteractionRIA\_UBS] | For UBS: interaction of the bank with USIA and UBS |
| [TransferBD\_UBS] | For UBS: transfer of collected biometric personal data between information systems of financial market institutions in charge of processing of biometric personal data and UBS in cases set forth in part 18.23 of Article 14.1 of Federal Law No. 149-FZ |
| [ProcessingRIA\_CBS] | For CBS: processing of biometric personal data (excluding collection) as well as information on the degree of compliance in the information systems of financial market institutions to perform identification and (or) authentication in case of fulfillment of conditions set forth in parts 18.18 and 18.20 of Article 14.1 of Federal Law No. 149-FZ, dated 27 July 2006, ‘On Information, Information Technologies and the Protection of Information’ (hereinafter, Federal Law No. 149-FZ) |
| [TransferRIA\_CBS] | For CBS: transfer of biometric personal data of natural persons as well as information on the degree of their compliance to the information systems of financial market institutions to perform identification and (or) authentication using fixed technical facilities of structural subdivisions of financial institutions, mobile (portable) computer devices (tablets) owned by financial institutions, payment terminals, ATM |
| [DelegationRIA\_CBS] | For CBS: interaction of financial institutions, other institutions, individual entrepreneurs with information systems of financial market institutions to authenticate a natural person |

## REFERENCES

|  |  |
| --- | --- |
| [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. 187-FZ, dated 26 July 2017, ‘On Security of the Critical Information Infrastructure of the Russian Federation’ |
| [3] | Federal Law No. 161-FZ, dated 27 June 2011, ‘On the National Payment System’ |
| [4] | Federal Law No. 211-FZ, dated 20 July 2020, ‘On Consummation of Financial Transactions Using Financial Platform’ |
| [5] | Bank of Russia Regulation No. 683-P, dated 17 April 2019, ‘On Establishing Binding Requirements for Credit Inistitutions to Information Security upon Carrying out Banking Activity to Combat Funds Transfers Without Consent of the Client’ |
| [6] | Bank of Russia Regulation No. 719-P, dated 4 June 2020, ‘On Requirements to Information Security upon Funds Transfers and on the Procedure of the Bank of Russia's Control over Compliance with Requirements to Information Security upon Funds Transfers’ |
| [7] | Bank of Russia Regulation No. 757-P, dated 20 April 2021, ‘On Establishing Binding Requirements for Non-banking Financial Institutions to Ensure Information Security upon Carrying out Activity in the Field of Financial Markets to Combat Unlawful Financial Operations’ |
| [8] | Bank of Russia Regulation No. 802-P, dated 25 July 2022, ‘On Requirements for Protection of Information Within the Payment System of the Bank of Russia’ |
| [9] | Bank of Russia Regulation No. 787-P, dated 12 January 2022, ‘On Binding Requirements for Credit Institutions to Operational Reliability upon Carrying out Banking Activity to Ensure Continuous Provision of Banking Services’ |
| [10] | Bank of Russia Regulation No. 779-P, dated 15 November 2021, ‘On Establishing Binding Requirements for Non-banking Financial Institutions to Operational Reliability upon Carrying out Activities Provided for by Part 1 of Article 76.1 of Federal Law No. 86-FZ, dated 10 July 2022, ‘On the Central Bank of the Russian Federation (Bank of Russia)’, to Ensure Continuous Provision of Financial Services (Other than Banking Services)’ |
| [11] | Bank of Russia Regulation No. 716-P, dated 8 April 2020, ‘On Requirements to the Operational Risk Management System in a Credit Institution and Banking Group’ |
| [12] | The National Standard of the Russian Federation GOST R 57580.1-2017 ‘Safety of Financial (Banking) Operations. Protection of Information of Financial Institutions. Basic Structure of Organisational and Technical Measures’ |
| [13] | The National Standard of the Russian Federation GOST R 57580.3-2022 ‘Safety of Financial (Banking) Operations. Management of Information Security Threat Risk and Ensuring Operational Reliability. General Provisions’ |