Банк России

СТАНДАРТ БАНКА РОССИИ

СТО БР БФБО-1.5-2023

БЕЗОПАСНОСТЬ ФИНАНСОВЫХ (БАНКОВСКИХ) ОПЕРАЦИЙ

УПРАВЛЕНИЕ ИНЦИДЕНТАМИ, СВЯЗАННЫМИ С РЕАЛИЗАЦИЕЙ ИНФОРМАЦИОННЫХ УГРОЗ, И ИНЦИДЕНТАМИ ОПЕРАЦИОННОЙ НАДЕЖНОСТИ

О ФОРМАХ И СРОКАХ ВЗАИМОДЕЙСТВИЯ БАНКА РОССИИ С КРЕДИТНЫМИ ОРГАНИЗАЦИЯМИ, НЕКРЕДИТНЫМИ ФИНАНСОВЫМИ ОРГАНИЗАЦИЯМИ И СУБЪЕКТАМИ НАЦИОНАЛЬНОЙ ПЛАТЕЖНОЙ СИСТЕМЫ ПРИ ВЫЯВЛЕНИИ ИНЦИДЕНТОВ, СВЯЗАННЫХ С РЕАЛИЗАЦИЕЙ ИНФОРМАЦИОННЫХ УГРОЗ, И ИНЦИДЕНТОВ ОПЕРАЦИОННОЙ НАДЕЖНОСТИ

МОСКВА
2023

ПРЕДИСЛОВИЕ

1. РАЗРАБОТАН Банком России.

2. ПРИНЯТ И ВВЕДЕН В ДЕЙСТВИЕ приказом Банка России от «08» февраля 2023 года № ОД-215.

3. ВЗАМЕН СТО БР БФБО-1.5–2018.

ОГЛАВЛЕНИЕ

1. ОБЛАСТЬ ПРИМЕНЕНИЯ

Настоящий стандарт регламентирует формы и сроки взаимодействия кредитных организаций, некредитных финансовых организаций и субъектов национальной платежной системы (далее при совместном упоминании – участники информационного обмена) с Банком России в случаях, предусмотренных законодательством Российской Федерации, в том числе нормативными актами Банка России.

Область действия настоящего стандарта определяется требованиями законодательства Российской Федерации, в том числе нормативных актов Банка России, которыми предусмотрены обязанности участников информационного обмена по информированию Банка России:

- о выявленных случаях и (или) попытках осуществления переводов денежных средств без согласия клиента, о случаях и (или) попытках осуществления операций, направленных на совершение финансовых сделок с использованием финансовой платформы без волеизъявления участника финансовой платформы, инцидентах защиты информации, в том числе незаконном раскрытии банковской тайны, персональных данных и (или) иных данных клиентов или работников участника информационного обмена, компьютерных инцидентах, компьютерных атаках и уязвимостях информационной безопасности, которые могут привести к инциденту защиты информации или компьютерному инциденту (далее при совместном упоминании – инциденты, связанные с реализацией информационных угроз);
- о событиях операционного риска или серии связанных событий операционного риска, вызванных информационными угрозами и (или) сбоями объектов информационной инфраструктуры, которые привели к неоказанию или ненадлежащему оказанию банковских или финансовых услуг – событиях операционного риска, связанных с нарушением операционной надежности (далее – инциденты операционной надежности);
- о планируемых публичных мероприятиях и мероприятиях по раскрытию информации, включая выпуск пресс-релизов и проведение пресс-конференций, размещение информации на официальных сайтах в сети Интернет, в отношении выявленных инцидентов защиты информации и инцидентов операционной надежности (далее – планируемые мероприятия по раскрытию информации).

Также настоящий стандарт применяется в рамках информационного обмена с участниками информационного обмена в соответствии с полномочиями Банка России в части направления запросов и получения необходимой информации о деятельности участников информационного обмена в соответствии с законодательством Российской Федерации, в том числе нормативными актами Банка России.

Объектом настоящего стандарта является следующее:

- Сведения обо всех случаях и (или) попытках осуществления переводов денежных средств без согласия клиента согласно требованиям:
  - Федерального закона от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе» (далее – Федеральный закон № 161-ФЗ) [3];
  - нормативного акта Банка России, устанавливающего форму и порядок направления операторами по переводу денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры, операторами электронных платформ в Банк России информации обо всех случаях и (или) попытках осуществления переводов денежных средств без согласия клиента, форме и порядке получения ими от Банка России информации, содержащейся в базе данных о случаях и попытках осуществления переводов денежных средств без согласия клиента, а также о порядке реализации операторами по переводу денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры, операторами электронных платформ мероприятий по противодействию осуществлению переводов денежных средств без согласия

клиента, разработанного на основании частей 4, 6 и 7 статьи 27 Федерального закона № 161-ФЗ [3].

- Сведения обо всех случаях и (или) попытках осуществления операций, направленных на совершение финансовых сделок с использованием финансовой платформы без волеизъявления участников финансовой платформы, согласно требованиям:
  - Федерального закона от 20 июля 2020 года № 211-ФЗ «О совершении финансовых сделок с использованием финансовой платформы» (далее – Федеральный закон № 211-ФЗ) [4];
  - нормативного акта Банка России, устанавливающего форму и порядок направления операторами финансовых платформ в Банк России информации обо всех случаях и (или) о попытках осуществления операций, направленных на совершение финансовых сделок с использованием финансовой платформы без волеизъявления участников финансовой платформы, и получения операторами финансовых платформ, финансовыми организациями от Банка России информации, содержащейся в базе данных о случаях и попытках осуществления операций, направленных на совершение финансовых сделок с использованием финансовой платформы без волеизъявления участников финансовой платформы, а также порядок реализации операторами финансовых платформ мероприятий по выявлению операций, направленных на совершение финансовых сделок с использованием финансовой платформы без волеизъявления участников финансовой платформы, и противодействию в совершении таких сделок на основании частей 2, 4 и 5 статьи 12 Федерального закона № 211-ФЗ [4].
- Сведения о выявлении инцидентов защиты информации, в том числе незаконного раскрытия банковской тайны, персональных данных и (или) иных данных клиентов или работников участника информационного обмена, согласно требованиям:
  - нормативного акта Банка России, устанавливающего обязательные для кредитных организаций требования к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента на основании статьи 57.4 Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» (далее – Федеральный закон № 86-ФЗ) [1];
  - нормативного акта Банка России, устанавливающего обязательные для некредитных финансовых организаций требования к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций на основании статьи 76.4–1 Федерального закона № 86-ФЗ [1];
  - нормативного акта Банка России, устанавливающего требования к обеспечению защиты информации при осуществлении переводов денежных средств и порядок осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств на основании части 3 статьи 27 Федерального закона № 161-ФЗ [3].
- Сведения о выявлении инцидентов операционной надежности согласно требованиям:
  - нормативного акта Банка России, устанавливающего обязательные для кредитных организаций требования к операционной надежности при осуществлении банковской деятельности в целях обеспечения непрерывности оказания банковских услуг на основании статьи 57.5 Федерального закона № 86-ФЗ [1];
  - нормативного акта Банка России, устанавливающего обязательные для некредитных финансовых организаций требования к операционной надежности при осуществлении деятельности в сфере финансовых рынков в целях обеспечения непрерывности оказания финансовых услуг (за исключением банковских услуг) на основании статьи 76.4-2 Федерального закона № 86-ФЗ [1].

- Сведения о компьютерных инцидентах, компьютерных атаках и уязвимостях информационной безопасности согласно требованиям:
  - Федерального закона от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (далее – Федеральный закон № 187-ФЗ) [2];
  - порядка информирования федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры;
  - нормативного акта Банка России, устанавливающего форму и порядок направления операторами по переводу денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры, операторами электронных платформ в Банк России информации обо всех случаях и (или) попытках осуществления переводов денежных средств без согласия клиента, форме и порядке получения ими от Банка России информации, содержащейся в базе данных о случаях и попытках осуществления переводов денежных средств без согласия клиента, а также о порядке реализации операторами по переводу денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры, операторами электронных платформ мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента, разработанного на основании частей 4, 6 и 7 статьи 27 Федерального закона № 161-ФЗ [3].
- Сведения от участников информационного обмена, использующих сервис срочного перевода и сервис несрочного перевода (далее – ССНП) для осуществления перевода денежных средств, о приостановлении/отмене приостановления обмена электронными сообщениями при выявлении инцидентов защиты информации при осуществлении переводов денежных средств на объектах информационной инфраструктуры участников информационного обмена согласно требованиям нормативного акта Банка России, устанавливающего требования к защите информации в платежной системе Банка России на основании пункта 19 части 1 и части 9 статьи 20 Федерального закона № 161-ФЗ [3].
- Сведения о планируемых мероприятиях по раскрытию информации о выявленных инцидентах защиты информации и инцидентах операционной надежности согласно требованиям:
  - нормативного акта Банка России, устанавливающего обязательные для кредитных организаций требования к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента на основании статьи 57.4 Федерального закона № 86-ФЗ [1];
  - нормативного акта Банка России, устанавливающего обязательные для некредитных финансовых организаций требования к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций на основании статьи 76.4–1 Федерального закона № 86-ФЗ [1];
  - нормативного акта Банка России, устанавливающего требования к обеспечению защиты информации при осуществлении переводов денежных средств и порядок осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств на основании части 3 статьи 27 Федерального закона № 161-ФЗ [3];

- нормативного акта Банка России, устанавливающего обязательные для кредитных организаций требования к операционной надежности при осуществлении банковской деятельности в целях обеспечения непрерывности оказания банковских услуг на основании статьи 57.5 Федерального закона № 86-ФЗ [1];
- нормативного акта Банка России, устанавливающего обязательные для некредитных финансовых организаций требования к операционной надежности при осуществлении деятельности в сфере финансовых рынков в целях обеспечения непрерывности оказания финансовых услуг (за исключением банковских услуг) на основании статьи 76.4-2 Федерального закона № 86-ФЗ [1].

Положения настоящего стандарта носят рекомендательный характер, если только обязательность применения отдельных из них не установлена законодательством Российской Федерации или нормативными актами Банка России. Настоящий стандарт может быть использован для включения отсылок на него и (или) прямого использования устанавливаемых в нем положений во внутренних документах финансовых организаций, а также в договорах и соглашениях, заключенных между организациями.

2. ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ, ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

В настоящем стандарте применены термины и определения следующих актов законодательства Российской Федерации и стандартов:

- в части общей терминологии используются термины и определения Национального стандарта Российской Федерации ГОСТ Р 57580.3-2022 «Безопасность финансовых (банковских) операций. Управление риском реализации информационных угроз и обеспечение операционной надежности. Общие положения» (далее – ГОСТ Р 57580.3-2022) [13] и Национального стандарта Российской Федерации ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» (далее – ГОСТ Р 57580.1-2017) [12];
- в части выявленных случаев и (или) попыток осуществления переводов денежных средств без согласия клиента, а также приостановления/отмены приостановления обмена электронными сообщениями при выявлении инцидентов защиты информации при осуществлении переводов денежных средств на объектах информационной инфраструктуры участников информационного обмена используются термины и определения Федерального закона № 161-ФЗ [3];
- в части выявленных случаев и (или) попыток осуществления операций, направленных на совершение финансовых сделок с использованием финансовой платформы без волеизъявления участника финансовой платформы, используются термины и определения Федерального закона № 211-ФЗ [4];
- в части выявленных инцидентов операционной надежности используются термины и определения Положения Банка России от 12 января 2022 года № 787-П «Об обязательных для кредитных организаций требованиях к операционной надежности при осуществлении банковской деятельности в целях обеспечения непрерывности оказания банковских услуг» (далее) (далее – Положение Банка России № 787-П) [9] и Положения Банка России от 15 ноября 2021 года № 779-П «Об установлении обязательных для некредитных финансовых организаций требований к операционной надежности при осуществлении видов деятельности, предусмотренных частью первой статьи 76.1 Федерального закона от 10 июля 2002 года N 86-ФЗ «О Центральном банке Российской Федерации (Банке России)», в целях обеспечения непрерывности оказания финансовых услуг (за исключением банковских услуг)» (далее – Положения Банка России № 779-П) [10];
- в части выявленных компьютерных инцидентов используются термины и определения Федерального закона № 187-ФЗ [2].

Также в настоящем стандарте используются следующие обозначения и сокращения:

АСОИ ФинЦЕРТ – техническая инфраструктура (автоматизированная система) Банка России;

АС «Фид-Антифрод» – Централизованная база данных о случаях и попытках осуществления переводов денежных средств без согласия клиента;

БДУ ФСТЭК – Банк данных угроз безопасности информации ФСТЭК России;

БД – база данных;

БИК – банковский идентификационный код;

ВПО – вредоносное программное обеспечение;

ДБО – дистанционное банковское обслуживание;

ДУЛ – документ, удостоверяющий личность;

ЕБС – единая биометрическая система;

ИНН – индивидуальный номер налогоплательщика;

КА – компьютерная атака;

КИ – компьютерный инцидент;

КИИ – критическая информационная инфраструктура;

МПС – международная платежная система;

НКЦКИ – Национальный координационный центр по компьютерным инцидентам;

ОПДС – оператор по переводу денежных средств;

ОЭП – оператор электронной платформы;

ПС – платежная система;

СБП – Система быстрых платежей;

Интернет – информационно-телекоммуникационная сеть «Интернет»;

СНИЛС – страховой номер индивидуального лицевого счета застрахованного лица в системе персонифицированного учета Фонда пенсионного и социального страхования Российской Федерации;

ТСП – торгово-сервисное предприятие;

ФЛ – физическое лицо;

ЮЛ – юридическое лицо;

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.

3. ВЗАИМОДЕЙСТВИЕ БАНКА РОССИИ С УЧАСТНИКАМИ ИНФОРМАЦИОННОГО ОБМЕНА

1. Участники информационного обмена информируют Банк России об инцидентах, связанных с реализацией информационных угроз, об инцидентах операционной надежности, о планируемых мероприятиях по раскрытию информации в случаях, предусмотренных законодательством Российской Федерации, в том числе нормативными актами Банка России.
2. Участники информационного обмена взаимодействуют с Банком России в соответствии со способами взаимодействия, описанными в разделе 4.
3. Условия и сроки информирования Банка России об инцидентах, связанных с реализацией информационных угроз, об инцидентах операционной надежности, о планируемых мероприятиях по раскрытию, а также направления ответов на запросы Банка России определяются настоящим стандартом в части, не урегулированной законодательством Российской Федерации и Банка России.
4. В настоящем стандарте определены формы представления данных, используемые для взаимодействия с Банком России в определенных законодательством Российской Федерации, в том числе нормативными актами Банка России, случаях направления в Банк России и получения от Банка России информации (в том числе по форме уведомления о представлении информации, форме уведомления о направлении запроса об исключении информации, форме уведомления о представлении ответа на запрос, форме уведомления о распространяемых данных, форме уведомления о событии). Содержание форм представления данных, направляемых в Банк России при информировании об инцидентах, связанных с реализацией информационных угроз, об инцидентах операционной надежности, о планируемых мероприятиях по раскрытию информации, а также ответов на запросы Банка России определяются настоящим стандартом.
5. В настоящем стандарте используется следующая схема наименования форм предоставления данных: <Тип формы представления данных>_<Объект, к которому применяется форма представления данных>_<Дополнительная классификация в рамках объекта>.

   <Тип формы представления данных> может принимать следующие значения:
   - NTF – форма представления данных, используемая участниками информационного обмена для уведомления Банка России. Не предусматривает предоставления формализованного ответа;
   - REQ – форма представления запроса, используемая участниками информационного обмена или Банком России для запроса сведений. Предусматривает обязательный формализованный ответ;
   - RESP – форма представления ответа на запрос, используемая участниками информационного обмена или Банком России для представления формализованного ответа на запрос сведений.

<Объект, к которому применяется форма представления данных> может принимать следующие значения:

- OWC – перевод денежных средств без согласия клиента или сделка с использованием финансовой платформы без волеизъявления участника финансовой платформы;
- ISI – инцидент защиты информации;
- ORI – инцидент операционной надежности;
- CI – компьютерный инцидент;
- CA – компьютерная атака;
- VLN – уязвимость информационной безопасности;
- IEP – участник информационного обмена.

<Дополнительная классификация в рамках объекта> зависит от объекта, к которому применяется форма представления данных, и приведена в разделах ниже.

6. Предзаполненные формы представления данных, используемые в настоящем стандарте, являются частным случаем форм представления данных и ориентированы на конкретную специфику (например, тип операции, инцидента и т.д.). Предзаполненные формы представления данных могут использоваться для информирования Банка России вместо основных форм представления данных.
7. Обязательность заполнения полей форм представления данных определяется в соответствии со следующими значениями:
   a. О – поле обязательно для заполнения;
   b. УО – поле обязательно для заполнения при выполнении заданного условия;
   c. Н – поле заполняется при наличии технической возможности получения данной информации.
8. Поля форм представления данных должны заполняться данными без использования методов скрытия информации, в том числе шифрования, маскирования или хеширования, если в правилах заполнения не указано иное.
9. Состав данных, направляемых в Банк России, при информировании об инцидентах, связанных с реализацией информационных угроз, инцидентах операционной надежности, о планируемых мероприятиях по раскрытию информации, не должен включать в себя сведения, составляющие государственную тайну.

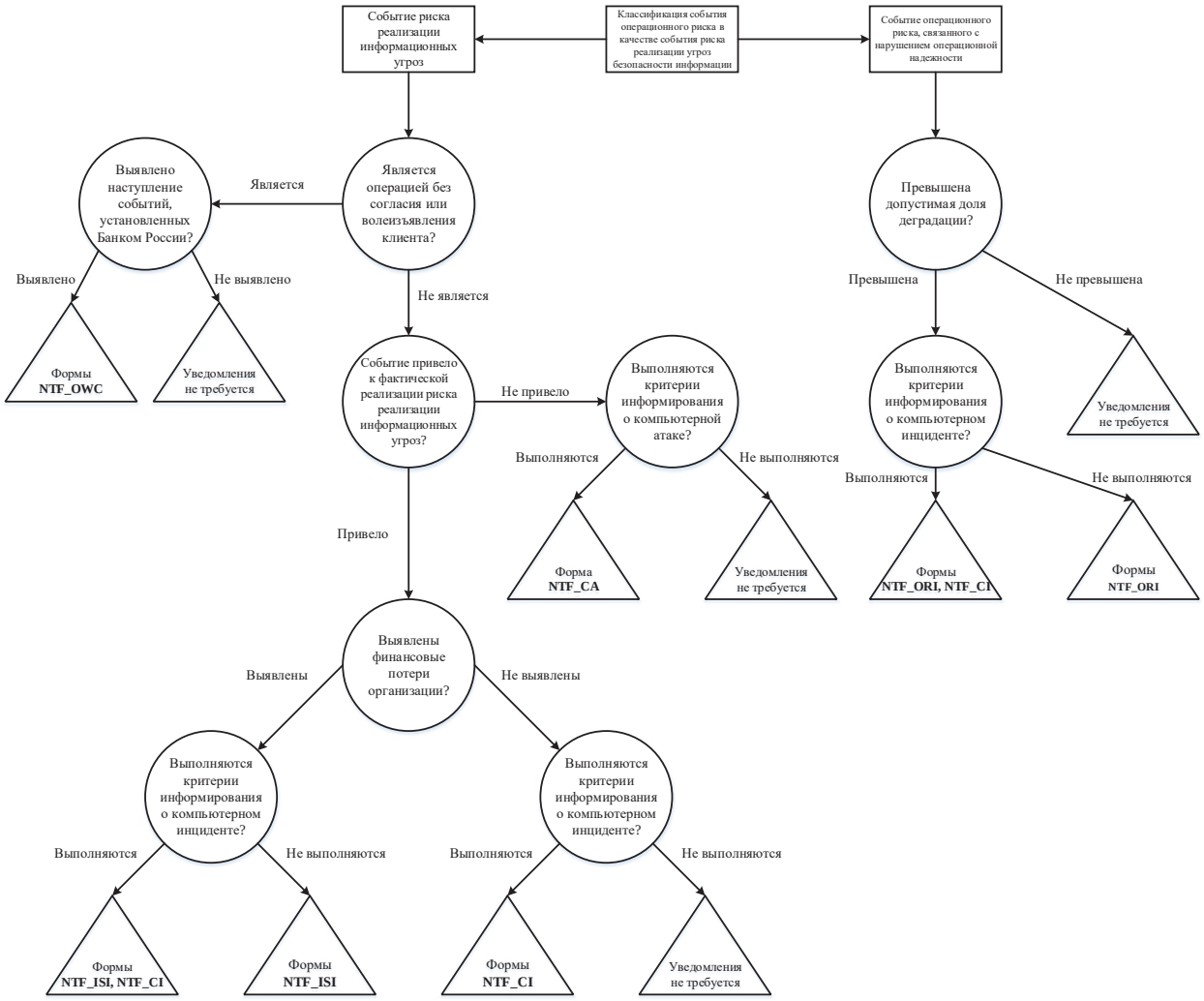
В настоящем стандарте описаны следующие формы представления данных:

Код формы представления данных	**Наименование формы представления данных**	**Раздел, в котором описана форма представления данных**
NTF_OWC_SNPS	Форма представления участниками информационного обмена – операторами по переводу денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры данных обо всех случаях и (или) попытках осуществления переводов денежных средств без согласия клиента	5.1 Приложение 1
NTF_OWC_OEP	Форма представления участниками информационного обмена – операторами электронных платформ данных обо всех случаях и (или) попытках осуществления переводов денежных средств без согласия клиента, включающих информацию об операциях по номинальному счету без согласия клиента-бенефициара	5.2 Приложение 2
NTF_OWC_OFP	Форма представления участниками информационного обмена – операторами финансовых платформ данных обо всех случаях и (или) попытках осуществления операций по финансовым сделкам без волеизъявления участника финансовой платформы	5.3 Приложение 3
REQ_OWC_Identification RESP_OWC_Identification	Форма запроса Банка России в целях идентификации получателя средств или плательщика, а также форма представления ответа Банку России	5.4 Приложение 4
REQ_OWC_UUID RESP_OWC_UUID	Форма запроса Банка России в целях получения данных об операции без согласия на основании сведений о совершенных противоправных действиях от федерального органа исполнительной власти в сфере внутренних дел, а также форма представления ответа Банку России	5.5 Приложение 5
REQ_OWC_Forward RESP_OWC_Forward	Форма запроса Банка России в целях получения данных о действиях участника информационного обмена, обслуживающего получателя средств, по переводу денежных средств, а также форма представления ответа Банку России	5.6 Приложение 6
REQ_OWC_Reverse RESP_OWC_Reverse	Форма запроса Банка России в целях получения информации о плательщиках указанному в запросе Банка России получателю средств, а также форма представления ответа Банку России	5.7 Приложение 7
REQ_OWC_Review RESP_OWC_Review	Форма запроса участника информационного обмена в случае необоснованного направления в Банк России информации о переводах без согласия клиента, а также форма представления ответа Банка России	5.8 Приложение 8
REQ_OWC_Correction RESP_OWC_Correction	Форма запроса Банка России о повторном направлении информации о переводах без согласия клиента, а также форма представления ответа Банку России	5.9 Приложение 9
NTF_OWC_DataUpdate	Форма представления участниками информационного обмена дополнительных и (или) уточняющих сведений по ранее направленной информации о переводах без согласия клиента	5.10 Приложение 10
NTF_ISI_Detect	Форма представления участниками информационного обмена данных о выявлении инцидента защиты информации	6.2 Приложение 12

NTF_ ISI _DataLeak	Форма представления участниками информационного обмена данных о выявлении незаконного раскрытия банковской тайны и (или) защищаемой информации в соответствии с нормативными актами Банка России	6.3 Приложение 13
NTF_ISI_Investigation	Форма представления участниками информационного обмена данных о результатах расследования инцидента защиты информации или незаконного раскрытия банковской тайны и (или) защищаемой информации в соответствии с нормативными актами Банка России	6.4 Приложение 14
REQ_ ISI _DataLeak RESP_ ISI _DataLeak	Форма запроса Банка России в целях подтверждения факта незаконного раскрытия банковской тайны и (или) защищаемой информации в соответствии с нормативными актами Банка России	6.5 Приложение 15
NTF_ORI_Detect	Форма представления участниками информационного обмена данных о выявлении инцидента операционной надежности	6.6 Приложение 16
NTF_ORI_Investigation	Форма представления участниками информационного обмена данных о результатах расследования инцидента операционной надежности	6.7 Приложение 17
NTF_CI	Форма представления участниками информационного обмена данных о компьютерных инцидентах	7.2 Приложение 19
NTF_CA	Форма представления участниками информационного обмена данных о компьютерных атаках	7.3 Приложение 21
NTF_VLN	Форма представления участниками информационного обмена данных о выявленных уязвимостях информационной безопасности	7.4 Приложение 23
REQ_IEP_Detect RESP_IEP_Detect	Форма запроса Банка России в целях получения сведений о выявленной компьютерной атаке или уязвимости информационной безопасности, а также форма представления ответа Банку России	7.5 Приложение 24
REQ_IEP_IsWebSite RESP_IEP_IsWebSite	Форма запроса Банка России в целях получения сведений о принадлежности участнику информационного обмена ресурса в сети Интернет, а также форма представления ответа Банку России	7.6 Приложение 25
REQ_IEP_CorrAccLock RESP_IEP_CorrAccLock	Форма запроса участника информационного обмена, использующего ССНП для осуществления перевода денежных средств, в целях приостановления/отмены приостановления обмена электронными сообщениями при выявлении инцидентов защиты информации при осуществлении переводов денежных средств с использованием ССНП на объектах информационной инфраструктуры участников информационного обмена, а также форма представления ответа Банка России	8 Приложение 26
NTF_IEP_Publication	Форма представления участниками информационного обмена сведений о планируемых мероприятиях по раскрытию информации о выявленных инцидентах защиты информации или инцидентах операционной надежности	9 Приложение 27

Для принятия решения об информировании участник информационного обмена может использовать схему принятия решений об информировании Банка России (рис. 1).

РИС. 1. СХЕМА ПРИНЯТИЯ РЕШЕНИЙ ОБ ИНФОРМИРОВАНИИ БАНКА РОССИИ О СОБЫТИЯХ РЕАЛИЗАЦИИ ИНФОРМАЦИОННЫХ УГРОЗ



4. СПОСОБЫ ВЗАИМОДЕЙСТВИЯ БАНКА РОССИИ И УЧАСТНИКОВ ИНФОРМАЦИОННОГО ОБМЕНА

Взаимодействие Банка России и участников информационного обмена осуществляется с использованием технической инфраструктуры (автоматизированной системы) Банка России – АСОИ ФинЦЕРТ.

В случае возникновения технической невозможности взаимодействия участников информационного обмена с Банком России с использованием АСОИ ФинЦЕРТ:

- участники информационного взаимодействия должны направлять информацию в Банк России с использованием контактной информации ФинЦЕРТ, размещенной на официальном сайте Банка России в информационно-телекоммуникационной сети «Интернет». Информация, направленная с использованием контактной информации ФинЦЕРТ, должна быть повторно направлена в Банк России при возобновлении технической возможности взаимодействия участников информационного обмена с Банком России с использованием АСОИ ФинЦЕРТ;
- Банк России направляет запросы участникам информационного взаимодействия с использованием контактной информации, предоставленной участником информационного обмена в карточке участника[1].

[1] Форма АСОИ ФинЦЕРТ, содержащая информацию об участнике информационного обмена.

5. ВЗАИМОДЕЙСТВИЕ УЧАСТНИКОВ ИНФОРМАЦИОННОГО ОБМЕНА С БАНКОМ РОССИИ В СЛУЧАЯХ (ИЛИ ПРИ ПОПЫТКАХ) ОСУЩЕСТВЛЕНИЯ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ БЕЗ СОГЛАСИЯ КЛИЕНТА, А ТАКЖЕ В СЛУЧАЯХ (ИЛИ ПРИ ПОПЫТКАХ) ОСУЩЕСТВЛЕНИЯ ОПЕРАЦИЙ, НАПРАВЛЕННЫХ НА СОВЕРШЕНИЕ ФИНАНСОВЫХ СДЕЛОК С ИСПОЛЬЗОВАНИЕМ ФИНАНСОВОЙ ПЛАТФОРМЫ, БЕЗ ВОЛЕИЗЪЯВЛЕНИЯ УЧАСТНИКА ФИНАНСОВОЙ ПЛАТФОРМЫ

5.1. ПРЕДСТАВЛЕНИЕ УЧАСТНИКАМИ ИНФОРМАЦИОННОГО ОБМЕНА – ОПЕРАТОРАМИ ПО ПЕРЕВОДУ ДЕНЕЖНЫХ СРЕДСТВ, ОПЕРАТОРАМИ ПЛАТЕЖНЫХ СИСТЕМ, ОПЕРАТОРАМИ УСЛУГ ПЛАТЕЖНОЙ ИНФРАСТРУКТУРЫ В БАНК РОССИИ ДАННЫХ ОБО ВСЕХ СЛУЧАЯХ И (ИЛИ) ПОПЫТКАХ ОСУЩЕСТВЛЕНИЯ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ БЕЗ СОГЛАСИЯ КЛИЕНТА

События, при наступлении которых участники информационного обмена – операторы по переводу денежных средств, операторы платежных систем, операторы услуг платежной инфраструктуры должны направлять в Банк России данные обо всех случаях и (или) попытках осуществления переводов денежных средств без согласия клиента (далее – информация о переводах без согласия клиента), а также сроки направления указанной информации установлены нормативным актом Банка России в соответствии с частями 4, 6 и 7 статьи 27 Федерального закона № 161-ФЗ [3].

Форма представления участниками информационного обмена – операторами по переводу денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры данных о переводах без согласия клиента (*NTF_OWC_SNPS*) в Банк России приведена в приложении 1 к настоящему стандарту.

5.2. ПРЕДСТАВЛЕНИЕ УЧАСТНИКАМИ ИНФОРМАЦИОННОГО ОБМЕНА – ОПЕРАТОРАМИ ЭЛЕКТРОННЫХ ПЛАТФОРМ В БАНК РОССИИ ДАННЫХ ОБО ВСЕХ СЛУЧАЯХ И (ИЛИ) ПОПЫТКАХ ОСУЩЕСТВЛЕНИЯ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ БЕЗ СОГЛАСИЯ КЛИЕНТА, ВКЛЮЧАЮЩИХ ИНФОРМАЦИЮ ОБ ОПЕРАЦИЯХ ПО НОМИНАЛЬНОМУ СЧЕТУ БЕЗ СОГЛАСИЯ КЛИЕНТА-БЕНЕФИЦИАРА

События, при наступлении которых участники информационного обмена – операторы электронных платформ должны направлять в Банк России данные обо всех случаях и (или) попытках осуществления переводов денежных средств без согласия клиента, включающие информацию об операциях по номинальному счету без согласия клиента – бенефициара (далее – информация о переводах без согласия клиента, включающая информацию об операциях по номинальному счету без согласия клиента-бенефициара), а также сроки направления указанной информации установлены нормативным актом Банка России в соответствии с частями 4, 6 и 7 статьи 27 Федерального закона № 161-ФЗ [3].

Форма представления участниками информационного обмена – операторами электронных платформ информации о переводах без согласия клиента, включающей информацию об операциях по номинальному счету без согласия клиента-бенефициара (*NTF_OWC_OEP*) в Банк России приведена в приложении 2 к настоящему стандарту.

5.3. ПРЕДСТАВЛЕНИЕ УЧАСТНИКАМИ ИНФОРМАЦИОННОГО ОБМЕНА – ОПЕРАТОРАМИ ФИНАНСОВЫХ ПЛАТФОРМ В БАНК РОССИИ ДАННЫХ ОБО ВСЕХ СЛУЧАЯХ И (ИЛИ) ПОПЫТКАХ ОСУЩЕСТВЛЕНИЯ ОПЕРАЦИЙ, НАПРАВЛЕННЫХ НА СОВЕРШЕНИЕ ФИНАНСОВЫХ СДЕЛОК С ИСПОЛЬЗОВАНИЕМ ФИНАНСОВОЙ ПЛАТФОРМЫ, БЕЗ ВОЛЕИЗЪЯВЛЕНИЯ УЧАСТНИКОВ ФИНАНСОВОЙ ПЛАТФОРМЫ

События, при наступлении которых участники информационного обмена – операторы финансовых платформ должны направлять в Банк России обо всех случаях и (или) попытках осуществления операций, направленных на совершение финансовых сделок с использованием финансовой платформы, без волеизъявления участника финансовой платформы (далее – операции по финансовым сделкам без волеизъявления участников финансовой платформы),

а также сроки направления указанной информации установлены нормативным актом Банка России в соответствии с частями 2, 4 и 5 статьи 12 Федерального закона № 211-ФЗ.

Форма представления участниками информационного обмена – операторами финансовых платформ данных обо всех случаях и (или) попытках осуществления операций по финансовым сделкам без волеизъявления участника финансовой платформы (*NTF_OWC_OFP*) в Банк России приведена в приложении 3 к настоящему стандарту.

5.4. ЗАПРОС БАНКА РОССИИ В ЦЕЛЯХ ИДЕНТИФИКАЦИИ ПОЛУЧАТЕЛЯ СРЕДСТВ ИЛИ ПЛАТЕЛЬЩИКА

Запрос Банка России к участнику информационного обмена направляется Банком России при получении от участника информационного обмена уведомления, содержащего информацию о переводах без согласия клиента, в целях идентификации получателя средств или плательщика в соответствии с частями 4, 6 и 7 статьи 27 Федерального закона № 161-ФЗ [3].

При получении запроса в целях идентификации получателя средств или плательщика участники информационного обмена направляют информацию в Банк России в сроки, установленные нормативным актом Банка России в соответствии с частями 4, 6 и 7 статьи 27 Федерального закона № 161-ФЗ [3].

Форма запроса Банка России, направляемого участнику информационного обмена в целях идентификации получателя средств или плательщика (*REQ_OWC_Identification*), а также форма представления ответа Банку России, содержащего информацию, идентифицирующую получателя средств или плательщика (*RESP_OWC_Identification*), приведены в приложении 4 к настоящему стандарту.

5.5. ЗАПРОС БАНКА РОССИИ В ЦЕЛЯХ ПОЛУЧЕНИЯ ДАННЫХ ОБ ОПЕРАЦИИ БЕЗ СОГЛАСИЯ НА ОСНОВАНИИ СВЕДЕНИЙ О СОВЕРШЕННЫХ ПРОТИВОПРАВНЫХ ДЕЙСТВИЯХ ОТ ФЕДЕРАЛЬНОГО ОРГАНА ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ В СФЕРЕ ВНУТРЕННИХ ДЕЛ

Запрос Банка России оператору по переводу денежных средств (уведомление от Банка России) направляется Банком России при получении от федерального органа исполнительной власти в сфере внутренних дел сведений о совершенных противоправных действиях.

При получении запроса оператор по переводу денежных средств направляет следующие формы представления данных в соответствии с указанными сроками:

- форму представления данных *NTF_OWC_SNPS* в сроки, установленные нормативным актом Банка России в соответствии с частями 4, 6 и 7 статьи 27 Федерального закона № 161-ФЗ [3], в случае классификации операции по переводу денежных средств, информация о которой получена от Банка России на основании сведений федерального органа исполнительной власти в сфере внутренних дел о совершенных противоправных действиях, как операции без согласия клиента;
- форму *RESP_OWC_UUID* в течение рабочего дня, следующего за днем получения запроса Банка России, в случае если на основании сведений из запроса Банка России операция по переводу денежных средств не была классифицирована как операция без согласия клиента или форма представления данных *NTF_OWC_SNPS* по соответствующей операции была направлена в Банк России ранее.

Форма запроса Банка России, направляемого оператору по переводу денежных средств, в целях получения данных об операции без согласия (*REQ_OWC_UUID*), а также форма представления ответа Банку России (*RESP_OWC_UUID*), направляемая в случае, предусмотренном абзацем 4 раздела 5.5 настоящего стандарта, приведены в приложении 5 к настоящему стандарту.

5.6. ЗАПРОС БАНКА РОССИИ В ЦЕЛЯХ ПОЛУЧЕНИЯ ДАННЫХ О ДЕЙСТВИЯХ УЧАСТНИКА ИНФОРМАЦИОННОГО ОБМЕНА, ОБСЛУЖИВАЮЩЕГО ПОЛУЧАТЕЛЯ СРЕДСТВ, ПО ПЕРЕВОДУ ДЕНЕЖНЫХ СРЕДСТВ

Запрос Банка России к участнику информационного обмена, обслуживающему получателя средств, направляется Банком России при получении уведомления или информации об осуществлении перевода денежных средств без согласия клиента в целях получения информации о действиях по дальнейшему переводу денежных средств получателем средств в соответствии с частями 4, 6 и 7 статьи 27 Федерального закона № 161-ФЗ [3].

При получении запроса от Банка России участник информационного обмена, обслуживающий получателя средств, направляет информацию о действиях по дальнейшему переводу денежных средств получателя средств в Банк России в сроки, установленные нормативным актом Банка России в соответствии с частями 4, 6 и 7 статьи 27 Федерального закона № 161-ФЗ [3].

Форма запроса Банка России, направляемого участнику информационного обмена, обслуживающему получателя средств, в целях получения данных о его действиях по переводу денежных средств (*REQ_OWC_Forward*), а также форма для представления ответа Банку России, содержащего информацию о действиях участника информационного обмена по переводу денежных средств (*RESP_OWC_Forward*), приведены в приложении 6 к настоящему стандарту.

5.7. ЗАПРОС БАНКА РОССИИ В ЦЕЛЯХ ПОЛУЧЕНИЯ ИНФОРМАЦИИ О ПЛАТЕЛЬЩИКАХ УКАЗАННОМУ В ЗАПРОСЕ БАНКА РОССИИ ПОЛУЧАТЕЛЮ СРЕДСТВ

Запрос Банка России к участнику информационного обмена, обслуживающему получателя средств, направляется Банком России при получении от участника информационного обмена уведомления или информации об осуществлении перевода денежных средств без согласия клиента в целях получения информации о плательщиках указанному получателю средств в соответствии с частями 4, 6 и 7 статьи 27 Федерального закона № 161-ФЗ [3].

При получении запроса от Банка России участник информационного обмена, обслуживающий получателя средств, направляет информацию о плательщиках указанному получателю средств в Банк России в сроки, установленные нормативным актом Банка России в соответствии с частями 4, 6 и 7 статьи 27 Федерального закона № 161-ФЗ [3].

Форма запроса Банка России, направляемого участнику информационного обмена, обслуживающему получателя средств, в целях получения информации о плательщиках указанному получателю средств (*REQ_OWC_Reverse*), а также форма для представления ответа Банку России, содержащего информацию о плательщиках указанному получателю средств (*RESP_OWC_Reverse*), приведены в приложении 7 к настоящему стандарту.

5.8. ЗАПРОС УЧАСТНИКА ИНФОРМАЦИОННОГО ОБМЕНА В СЛУЧАЕ НЕОБОСНОВАННОГО НАПРАВЛЕНИЯ В БАНК РОССИИ ИНФОРМАЦИИ О ПЕРЕВОДАХ БЕЗ СОГЛАСИЯ КЛИЕНТА

Запрос участника информационного обмена направляется в Банк России при выявлении в рамках реализуемой участником информационного обмена системы управления рисками случаев необоснованного направления информации о переводах без согласия клиента по ранее направленному уведомлению в Банк России, в соответствии с частями 4, 6 и 7 статьи 27 Федерального закона № 161-ФЗ [3].

По итогам рассмотрения запроса Банк России направляет участнику информационного обмена информацию о рассмотрении запроса.

Форма запроса участника информационного обмена, направляемого в Банк России, в случае необоснованного направления в Банк России информации о переводах без согласия клиента (*REQ_OWC_Review*), а также форма для представления ответа участнику информационного обмена, используемая Банком России (*RESP_OWC_Review*), приведены в приложении 8 к настоящему стандарту.

5.9. ЗАПРОС БАНКА РОССИИ О ПОВТОРНОМ НАПРАВЛЕНИИ ИНФОРМАЦИИ О ПЕРЕВОДАХ БЕЗ СОГЛАСИЯ КЛИЕНТА

Запрос Банка России к участнику информационного обмена направляется Банком России при получении от участника информационного обмена уведомления или информации об осуществлении перевода денежных средств без согласия клиента с целью получения уточняющих сведений к ранее направленной в Банк России информации о переводах без согласия клиента, в соответствии с частями 4, 6 и 7 статьи 27 Федерального закона № 161-ФЗ [3].

При получении запроса от Банка России участник информационного обмена направляет повторную информацию о переводах без согласия клиента в сроки, установленные нормативным актом Банка России в соответствии с частями 4, 6 и 7 статьи 27 Федерального закона № 161-ФЗ [3].

Форма запроса Банка России, направляемого участнику информационного обмена, о повторном направлении информации о переводах без согласия клиента (*REQ_OWC_Correction*), а также форма для представления ответа Банку России, содержащего повторную информацию о переводах без согласия клиента у (*RESP_OWC_Correction*), приведены в приложении 9 к настоящему стандарту.

5.10. ПРЕДСТАВЛЕНИЕ УЧАСТНИКАМИ ИНФОРМАЦИОННОГО ОБМЕНА ДОПОЛНИТЕЛЬНЫХ И (ИЛИ) УТОЧНЯЮЩИХ СВЕДЕНИЙ ПО РАНЕЕ НАПРАВЛЕННОЙ ИНФОРМАЦИИ В БАНК РОССИИ

Условия, при наступлении которых участники информационного обмена направляют в Банк России дополнительные и (или) уточняющие сведения по ранее направленной информации в Банк России, также сроки направления указанной информации установлены нормативным актом Банка России в соответствии с частями 4, 6 и 7 статьи 27 Федерального закона № 161-ФЗ [3].

Форма представления участниками информационного обмена дополнительных и (или) уточняющих сведений по ранее направленной информации о переводах без согласия клиента в Банк России (*NTF_OWC_DataUpdate*) приведена в приложении 10 к настоящему стандарту.

Данная форма ориентирована на актуализацию сведений, находящихся в базе данных о случаях и попытках осуществления переводов денежных средств без согласия клиента:

- о закрытии банковского счета;
- о прекращении использования платежной карты;
- о прекращении действия договора абонентского обслуживания подвижной радиотелефонной связи;
- о прекращении использования электронного средства платежа;
- об изменении номера документа, удостоверяющего личность;
- об изменении абонентского номера подвижной радиотелефонной связи клиента.

5.11. СХЕМА ВЗАИМОДЕЙСТВИЯ БАНКА РОССИИ И УЧАСТНИКОВ ИНФОРМАЦИОННОГО ОБМЕНА ПРИ ВЫЯВЛЕНИИ СЛУЧАЕВ И (ИЛИ) ПОПЫТОК ОСУЩЕСТВЛЕНИЯ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ БЕЗ СОГЛАСИЯ КЛИЕНТА, А ТАКЖЕ ПРИ ВЫЯВЛЕНИИ СЛУЧАЕВ И (ИЛИ) ПОПЫТОК ОСУЩЕСТВЛЕНИЯ ОПЕРАЦИЙ, НАПРАВЛЕННЫХ НА СОВЕРШЕНИЕ ФИНАНСОВЫХ СДЕЛОК С ИСПОЛЬЗОВАНИЕМ ФИНАНСОВОЙ ПЛАТФОРМЫ БЕЗ ВОЛЕИЗЪЯВЛЕНИЯ УЧАСТНИКА ФИНАНСОВОЙ ПЛАТФОРМЫ

Схема взаимодействия Банка России и участников информационного обмена при выявленных случаях и (или) попытках осуществления переводов денежных средств без согласия клиента, а также при выявленных случаях и (или) попытках осуществления операций, направленных на совершение финансовых сделок с использованием финансовой платформы без волеизъявления участника финансовой платформы, представлена на рис. 2.

Схема взаимодействия Банка России и операторов по переводу денежных средств в связи с получением Банком России сведений о совершенных противоправных действиях от федерального органа исполнительной власти в сфере внутренних дел, представлена на рис. 3.

РИС. 2. СХЕМА ВЗАИМОДЕЙСТВИЯ БАНКА РОССИИ И УЧАСТНИКОВ ИНФОРМАЦИОННОГО ОБМЕНА ПРИ ВЫЯВЛЕНИИ СЛУЧАЕВ И (ИЛИ) ПОПЫТОК ОСУЩЕСТВЛЕНИЯ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ БЕЗ СОГЛАСИЯ КЛИЕНТА, А ТАКЖЕ ПРИ ВЫЯВЛЕНИИ СЛУЧАЕВ И (ИЛИ) ПОПЫТОК ОСУЩЕСТВЛЕНИЯ ОПЕРАЦИЙ, НАПРАВЛЕННЫХ НА СОВЕРШЕНИЕ ФИНАНСОВЫХ СДЕЛОК С ИСПОЛЬЗОВАНИЕМ ФИНАНСОВОЙ ПЛАТФОРМЫ БЕЗ ВОЛЕИЗЪЯВЛЕНИЯ УЧАСТНИКА ФИНАНСОВОЙ ПЛАТФОРМЫ

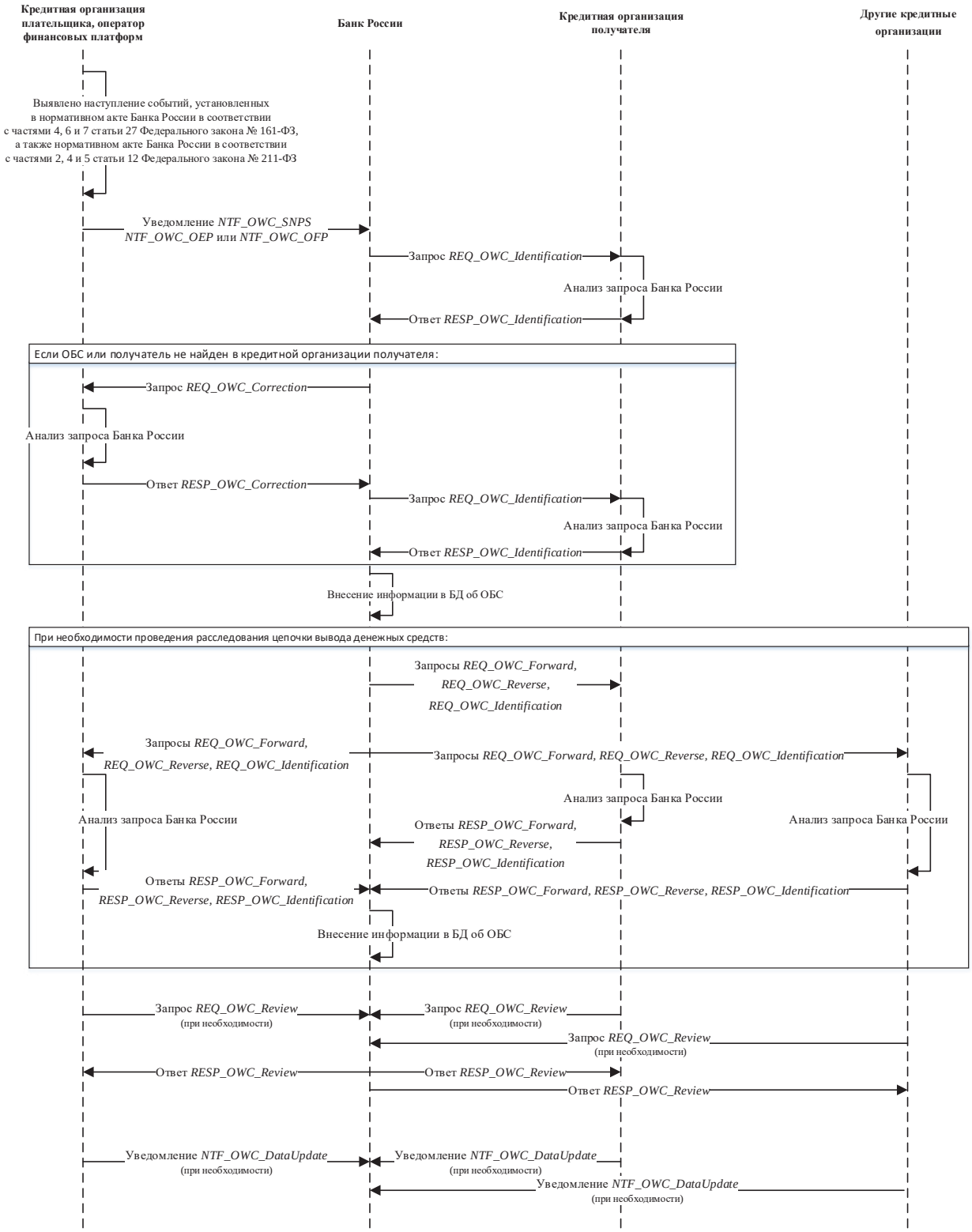
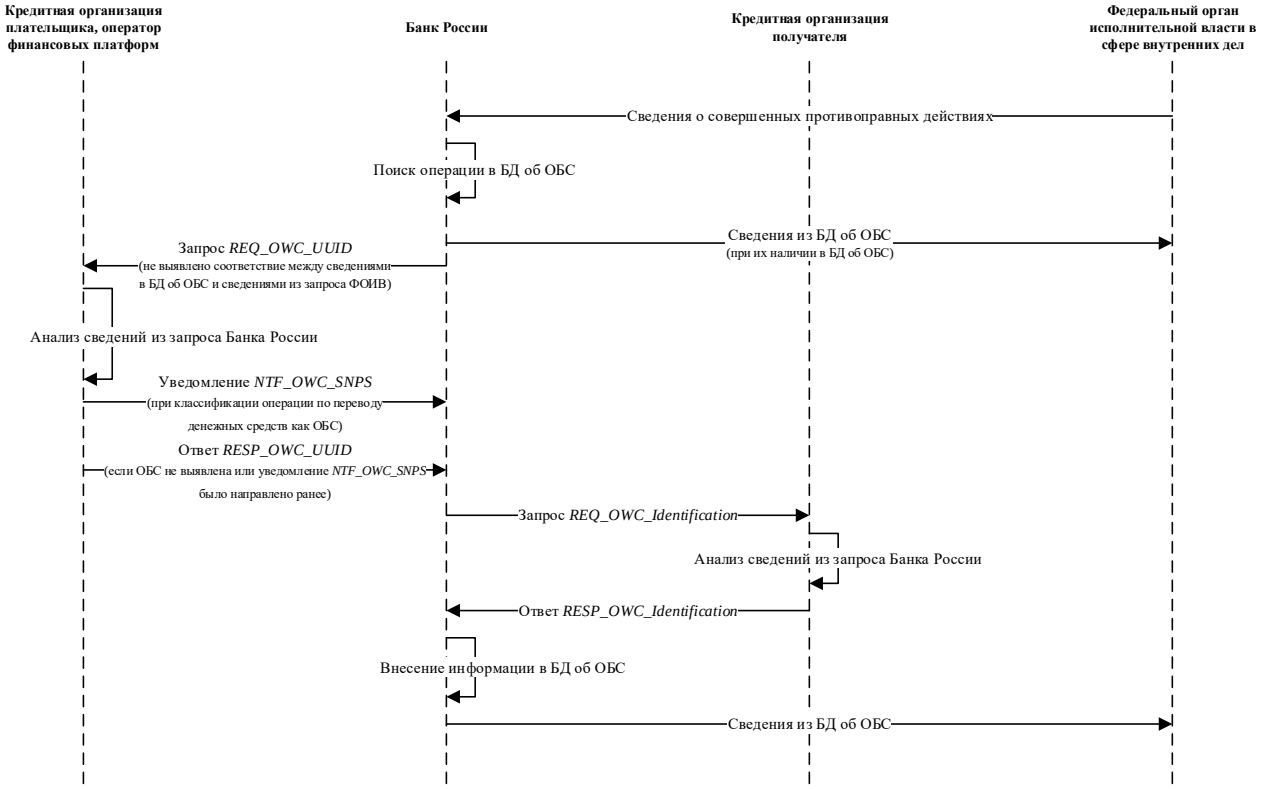


РИС. 3. СХЕМА ВЗАИМОДЕЙСТВИЯ БАНКА РОССИИ И ОПЕРАТОРОВ ПО ПЕРЕВОДУ ДЕНЕЖНЫХ СРЕДСТВ В СВЯЗИ С ПОЛУЧЕНИЕМ БАНКОМ РОССИИ СВЕДЕНИЙ О СОВЕРШЕННЫХ ПРОТИВОПРАВНЫХ ДЕЙСТВИЯХ ОТ ФЕДЕРАЛЬНОГО ОРГАНА ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ В СФЕРЕ ВНУТРЕННИХ ДЕЛ



6. ВЗАИМОДЕЙСТВИЕ УЧАСТНИКОВ ИНФОРМАЦИОННОГО ОБМЕНА С БАНКОМ РОССИИ ПРИ ВЫЯВЛЕНИИ ИНЦИДЕНТОВ ЗАЩИТЫ ИНФОРМАЦИИ, В ТОМ ЧИСЛЕ НЕЗАКОННОМ РАСКРЫТИИ БАНКОВСКОЙ ТАЙНЫ, ПЕРСОНАЛЬНЫХ ДАННЫХ И (ИЛИ) ИНЫХ ДАННЫХ КЛИЕНТОВ ИЛИ РАБОТНИКОВ УЧАСТНИКА ИНФОРМАЦИОННОГО ОБМЕНА, И ИНЦИДЕНТОВ ОПЕРАЦИОННОЙ НАДЕЖНОСТИ

6.1. ПЕРЕЧЕНЬ ТИПОВ ИНЦИДЕНТОВ ЗАЩИТЫ ИНФОРМАЦИИ, СОГЛАСОВАННЫЙ С ФЕДЕРАЛЬНЫМ ОРГАНОМ ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ, УПОЛНОМОЧЕННЫМ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ, И ИНЦИДЕНТОВ ОПЕРАЦИОННОЙ НАДЕЖНОСТИ В РАЗРЕЗЕ ВИДОВ ДЕЯТЕЛЬНОСТИ КРЕДИТНЫХ ОРГАНИЗАЦИЙ, НЕКРЕДИТНЫХ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ И СУБЪЕКТОВ НАЦИОНАЛЬНОЙ ПЛАТЕЖНОЙ СИСТЕМЫ И СОСТАВЛЯЮЩИХ ИХ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ

Участники информационного обмена в соответствии с абзацем восьмым пункта 8 Положения Банка России от 17 апреля 2019 года № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента» (далее – Положение Банка России № 683-П) [5], абзацем вторым пункта 1.15 Положения Банка России от 20 апреля 2021 года № 757-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций» (далее – Положение Банка России № 757-П) [7], абзацем вторым пункта 1.5 Положения Банка России от 4 июня 2020 года № 719-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств» (далее – Положение Банка России № 719-П) [6] должны информировать Банк России о выявленных инцидентах защиты информации, включенных в перечень типов инцидентов, согласованный с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности.

Участники информационного обмена в соответствии с абзацем вторым пункта 11 Положения Банка России № 787-П [9], абзацем вторым пункта 1.15 Положения Банка России № 779-П [10] должны информировать Банк России о выявленных инцидентах операционной надежности, включенных в перечень типов инцидентов операционной надежности.

Перечень типов инцидентов, согласованный с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, за исключением случаев незаконного раскрытия банковской тайны и (или) защищаемой информации, в соответствии с нормативными актами Банка России, и перечень типов инцидентов операционной надежности в разрезе видов деятельности кредитных организаций, некредитных финансовых организаций и субъектов национальной платежной системы и составляющих их технологических процессов (далее – перечень типов инцидентов защиты информации и инцидентов операционной надежности) приведены в приложении 11 к настоящему стандарту.

6.2. ПРЕДСТАВЛЕНИЕ УЧАСТНИКАМИ ИНФОРМАЦИОННОГО ОБМЕНА ДАННЫХ О ВЫЯВЛЕНИИ ИНЦИДЕНТА ЗАЩИТЫ ИНФОРМАЦИИ

Данные о выявлении инцидента защиты информации направляются участниками информационного обмена в Банк России в соответствии с абзацем восьмым пункта 8 Положения Банка России № 683-П [5], абзацем вторым пункта 1.15 Положения Банка России № 757-П [7] и абзацем вторым пункта 1.5 Положения Банка России № 719-П [6] при выявлении критериев информирования об инциденте защиты информации в соответствии с перечнем типов инцидентов защиты информации, приведенным в разделе 6.1.

При выявлении указанных критериев информирования участники информационного обмена направляют данные о выявлении инцидента защиты информации в соответствии со следующими сроками, если иное не предусмотрено нормативными актами Банка России:

- в течение 3 часов с момента выявления инцидента защиты информации для участников информационного взаимодействия, реализующих усиленный или стандартный уровень защиты информации в соответствии с ГОСТ Р 57580.1–2017 [12];
- в течение 24 часов с момента выявления инцидента защиты информации для остальных участников информационного взаимодействия.

Форма представления участниками информационного обмена данных о выявлении инцидента защиты информации (*NTF_ISI_Detect*) в Банк России приведена в приложении 12 к настоящему стандарту.

6.3. ПРЕДСТАВЛЕНИЕ УЧАСТНИКАМИ ИНФОРМАЦИОННОГО ОБМЕНА ДАННЫХ О ВЫЯВЛЕНИИ НЕЗАКОННОГО РАСКРЫТИЯ БАНКОВСКОЙ ТАЙНЫ И (ИЛИ) ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ В СООТВЕТСТВИИ С НОРМАТИВНЫМИ АКТАМИ БАНКА РОССИИ

Данные о выявлении незаконного раскрытия банковской тайны и (или) защищаемой информации в соответствии с нормативными актами Банка России направляются участниками информационного обмена в Банк России при выявлении участником информационного обмена факта незаконного раскрытия банковской тайны и (или) защищаемой информации в соответствии с абзацем вторым пункта 1.15 Положения Банка России № 757-П [7], абзацами первым и восьмым пункта 8 Положения Банка России № 683-П [5] с учетом положений пунктов 7.3 и 7.6 Положения Банка России от 08.04.2020 № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе» (далее – Положение Банка России № 716-П) [11], абзацем вторым пункта 1.5 Положения Банка России № 719-П [6], при условии что сведения о факте незаконного раскрытия персональных данных ранее не были направлены в Банк России в рамках взаимодействия участников информационного обмена с Банком России при выявлении компьютерных инцидентов, а также в случаях, предусмотренных разделом 6.5 настоящего стандарта.

При выявлении указанного критерия направления формы представления данных участники информационного обмена направляют данные о выявлении незаконного раскрытия банковской тайны и (или) защищаемой информации в соответствии со следующими сроками, если иное не предусмотрено нормативными актами Банка России:

- в течение 3 часов с момента выявления инцидента защиты информации для участников информационного взаимодействия, реализующих усиленный или стандартный уровни защиты информации в соответствии с ГОСТ Р 57580.1–2017 [12];
- в течение 24 часов с момента выявления инцидента защиты информации для остальных участников информационного взаимодействия.

Форма представления участниками информационного обмена данных о выявлении незаконного раскрытия банковской тайны и (или) защищаемой информации в соответствии с нормативными актами Банка России (*NTF_ISI_DataLeak*) приведена в приложении 13 к настоящему стандарту.

6.4. ПРЕДСТАВЛЕНИЕ УЧАСТНИКАМИ ИНФОРМАЦИОННОГО ОБМЕНА ДАННЫХ О РЕЗУЛЬТАТАХ РАССЛЕДОВАНИЯ ИНЦИДЕНТА ЗАЩИТЫ ИНФОРМАЦИИ ИЛИ НЕЗАКОННОГО РАСКРЫТИЯ БАНКОВСКОЙ ТАЙНЫ И (ИЛИ) ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ В СООТВЕТСТВИИ С НОРМАТИВНЫМИ АКТАМИ БАНКА РОССИИ

Данные о результатах расследования инцидента защиты информации или незаконного раскрытия банковской тайны и (или) защищаемой информации в соответствии с нормативными актами Банка России направляются участниками информационного обмена в Банк России в соответствии с абзацем вторым пункта 1.15 Положения Банка России № 757-П [7], абзаца-

ми первым и восьмым пункта 8 Положения Банка России № 683-П [5] с учетом положений пунктов 7.3 и 7.6 Положения Банка России № 716-П [11], абзацем вторым пункта 1.5 Положения Банка России № 719-П [6] в случаях, если ранее участником информационного обмена в Банк России была направлена форма представления данных о выявлении инцидента защиты информации или незаконного раскрытия банковской тайны и (или) защищаемой информации в соответствии с нормативными актами Банка России.

При выявлении указанного критерия направления формы представления данных участники информационного обмена направляют данные о результатах расследования инцидента защиты или незаконного раскрытия банковской тайны и (или) защищаемой информации в соответствии с нормативными актами Банка России в течение 30 дней с момента направления в Банк России формы представления данных о выявлении инцидента защиты информации или незаконного раскрытия банковской тайны и (или) защищаемой информации, если иное не предусмотрено нормативными актами Банка России.

Форма представления участниками информационного обмена данных о результатах расследования инцидента защиты информации или незаконного раскрытия банковской тайны и (или) защищаемой информации в соответствии с нормативными актами Банка России (*NTF_ISI_Investigation*) в Банк России, приведена в приложении 14 к настоящему стандарту.

6.5. ЗАПРОС БАНКА РОССИИ В ЦЕЛЯХ ПОДТВЕРЖДЕНИЯ ФАКТА НЕЗАКОННОГО РАСКРЫТИЯ БАНКОВСКОЙ ТАЙНЫ И (ИЛИ) ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ В СООТВЕТСТВИИ С НОРМАТИВНЫМИ АКТАМИ БАНКА РОССИИ

Запрос Банка России к участнику информационного обмена направляется Банком России в соответствии с законодательством Российской Федерации (в частности, в соответствии с абзацами первым и восьмым пункта 8 Положения Банка России № 683-П [5] с учетом положений пунктов 7.3 и 7.6 Положения Банка России № 716-П [11]) при выявлении факта незаконного раскрытия банковской тайны и (или) защищаемой информации в соответствии с нормативными актами Банка России в целях получения подтверждения факта незаконного раскрытия банковской тайны и (или) защищаемой информации в соответствии с нормативными актами Банка России.

При получении запроса в целях подтверждения факта незаконного раскрытия банковской тайны и (или) защищаемой информации в соответствии с нормативными актами Банка России, участники информационного обмена направляют следующие формы представления данных в соответствии с указанными сроками:

- форму представления данных *NTF_ISI_DataLeak* в течение 24 часов, в случае выявления на основании сведений из запроса Банка России факта незаконного раскрытия банковской тайны и (или) защищаемой информации в соответствии с нормативными актами Банка России;
- форму *RESP_ISI_DataLeak* в течение 24 часов, в случае если на основании сведений из запроса Банка России не был выявлен факт незаконного раскрытия банковской тайны и (или) защищаемой информации в соответствии с нормативными актами Банка России.

Форма запроса Банка России, направляемого участнику информационного обмена, в целях подтверждения факта незаконного раскрытия банковской тайны и (или) защищаемой информации в соответствии с нормативными актами Банка России (*REQ_ISI_DataLeak*), а также форма для представления ответа Банку России, содержащего информацию о не выявленном факте незаконного раскрытия банковской тайны и (или) защищаемой информации в соответствии с нормативными актами Банка России (*RESP_ISI_DataLeak*), направляемая в случае, предусмотренном абзацем 4 раздела 6.5 настоящего стандарта, приведены в приложении 15 к настоящему стандарту.

6.6. ПРЕДСТАВЛЕНИЕ УЧАСТНИКАМИ ИНФОРМАЦИОННОГО ОБМЕНА ДАННЫХ О ВЫЯВЛЕНИИ ИНЦИДЕНТА ОПЕРАЦИОННОЙ НАДЕЖНОСТИ

Данные о выявлении инцидента операционной надежности направляются участниками информационного обмена в Банк России в соответствии с абзацем вторым пункта 11 Положения Банка России № 787-П [9] и абзацем вторым пункта 1.15 Положения Банка России № 779-П [10] при выявлении критериев информирования об инциденте операционной надежности в соответствии с перечнем инцидентов защиты информации, приведенным в разделе 6.1.

При выявлении указанных критериев информирования участники информационного обмена направляют данные о выявлении инцидента операционной надежности в соответствии со следующими сроками, если иное не предусмотрено нормативными актами Банка России:

- в течение 3 часов с момента выявления инцидента операционной надежности для участников информационного взаимодействия, реализующих усиленный или стандартный уровни защиты информации в соответствии с ГОСТ Р 57580.1-2017 [12];
- в течение 24 часов с момента выявления инцидента операционной надежности для остальных участников информационного взаимодействия.

Форма представления участниками информационного обмена данных о выявлении инцидента операционной надежности (*NTF_ORI_Detect*) в Банк России приведена в приложении 16 к настоящему стандарту.

6.7. ПРЕДСТАВЛЕНИЕ УЧАСТНИКАМИ ИНФОРМАЦИОННОГО ОБМЕНА ДАННЫХ О РЕЗУЛЬТАТАХ РАССЛЕДОВАНИЯ ИНЦИДЕНТА ОПЕРАЦИОННОЙ НАДЕЖНОСТИ

Данные о результатах расследования инцидента операционной надежности направляются участниками информационного обмена в Банк России в соответствии с абзацем вторым пункта 11 Положения Банка России № 787-П [9] и абзацем вторым пункта 1.15 Положения Банка России № 779-П [10] в случаях, если ранее участником информационного обмена была направлена в Банк России форма представления данных о выявлении инцидента операционной надежности.

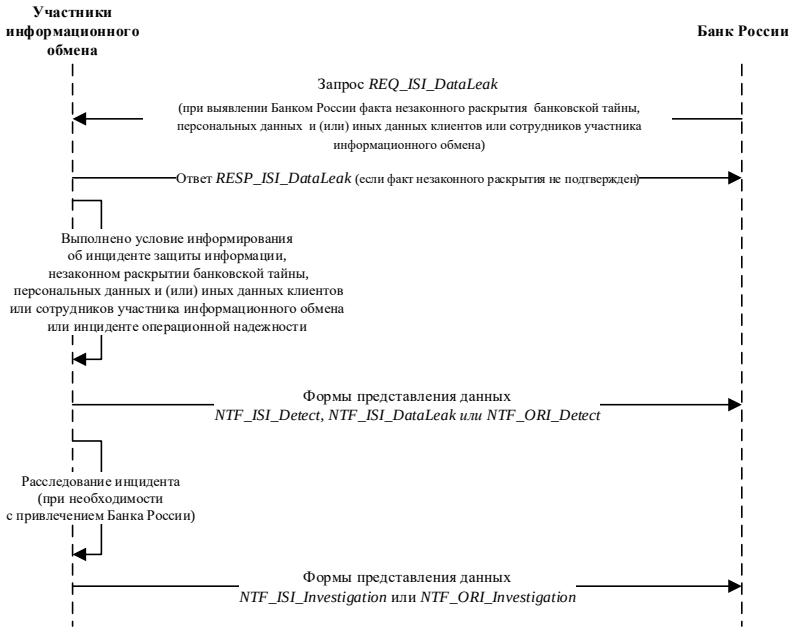
При выявлении указанного критерия направления формы представления данных участники информационного обмена направляют данные о результатах расследования инцидента операционной надежности в течение 30 дней с момента направления в Банк России формы представления данных о выявлении инцидента операционной надежности, если иное не предусмотрено нормативными актами Банка России.

Форма представления участниками информационного обмена данных о результатах расследования инцидента операционной надежности (*NTF_ORI_Investigation*) приведена в приложении 17 к настоящему стандарту.

Схема взаимодействия Банка России и участников информационного обмена при выявлении инцидентов защиты информации и инцидентов операционной надежности.

Схема взаимодействия Банка России и участников информационного обмена при выявлении инцидентов защиты информации и инцидентов операционной надежности представлена на рис. 4.

РИС. 4. СХЕМА ВЗАИМОДЕЙСТВИЯ БАНКА РОССИИ И УЧАСТНИКОВ ИНФОРМАЦИОННОГО ОБМЕНА ПРИ ВЫЯВЛЕНИИ ИНЦИДЕНТОВ ЗАЩИТЫ ИНФОРМАЦИИ И ИНЦИДЕНТОВ ОПЕРАЦИОННОЙ НАДЕЖНОСТИ



7. ВЗАИМОДЕЙСТВИЕ УЧАСТНИКОВ ИНФОРМАЦИОННОГО ОБМЕНА С БАНКОМ РОССИИ ПРИ ВЫЯВЛЕНИИ КОМПЬЮТЕРНЫХ ИНЦИДЕНТОВ, КОМПЬЮТЕРНЫХ АТАК И УЯЗВИМОСТЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

7.1. ПЕРЕЧЕНЬ КОМПЬЮТЕРНЫХ ИНЦИДЕНТОВ И КОМПЬЮТЕРНЫХ АТАК

Перечень компьютерных инцидентов и компьютерных атак, включающий критерии информирования о компьютерных инцидентах и компьютерных атаках, в соответствии с требованиями Федерального закона № 187-ФЗ [2], а также с частями 4, 6 и 7 статьи 27 Федерального закона № 161 ФЗ [3], абзацем восьмым пункта 8 Положения Банка России № 683-П [5], абзацем вторым пункта 1.15 Положения Банка России № 757-П [7] и абзацем вторым пункта 1.5 Положения Банка России № 719-П [6] приведен в приложении 18 к настоящему стандарту.

7.2. ПРЕДСТАВЛЕНИЕ УЧАСТНИКАМИ ИНФОРМАЦИОННОГО ОБМЕНА ДАННЫХ О КОМПЬЮТЕРНЫХ ИНЦИДЕНТАХ

Данные о компьютерных инцидентах направляются участниками информационного обмена в Банк России в соответствии с частью 2 статьи 9 Федерального закона № 187-ФЗ [2], пунктом 5 Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации, утв. приказом ФСБ России от 19 июня 2019 г. № 282 (далее – Порядок, утвержденный приказом ФСБ России № 282), абзацем восьмым пункта 8 Положения Банка России № 683-П [5], абзацем вторым пункта 1.15 Положения Банка России № 757-П [7] и абзацем вторым пункта 1.5 Положения Банка России № 719-П [6] при выявлении критериев информирования о компьютерном инциденте в соответствии с перечнем компьютерных инцидентов, приведенным в разделе 7.1, а также в случаях, предусмотренных разделом 7.5 настоящего стандарта.

При выявлении указанных критериев информирования участники информационного обмена направляют информацию о компьютерном инциденте в соответствии со следующими сроками:

- в течение 3 часов с момента выявления компьютерного инцидента в случае его связи с функционированием значимого объекта критической информационной инфраструктуры;
- в течение 24 часов с момента выявления компьютерного инцидента во всех иных случаях.

Форма представления участниками информационного обмена информации о компьютерных инцидентах (*NTF_CI*) приведена в приложении 19 к настоящему стандарту.

В приложении 20 приведены следующие формы представления данных, которые являются предзаполненными вариантами формы *NTF_ CI* и ориентированы на конкретные типы компьютерных инцидентов в соответствии с перечнем компьютерных инцидентов:

- форма представления данных *NTF_CI_DoS*, используемая участниками информационного обмена для уведомления Банка России о компьютерном инциденте – замедлении работы ресурса в результате атаки типа «Отказ в обслуживании»;
- форма представления данных *NTF_CI_ApplicationCompromise*, используемая участниками информационного обмена для уведомления Банка России о компьютерном инциденте – успешной эксплуатации уязвимости ресурса;
- форма представления данных *NTF_CI_MalwareInfection*, используемая участниками информационного обмена для уведомления Банка России о компьютерном инциденте – заражении вирусным программным обеспечением;
- форма представления данных *NTF_CI_AccountCompromise*, используемая участниками информационного обмена для уведомления Банка России о компьютерном инциденте – компрометации учетной записи;

- форма представления данных *NTF_CI_PhishingContent*, используемая участниками информационного обмена для уведомления Банка России о компьютерном инциденте – использовании контролируемого ресурса для фишинга;
- форма представления данных *NTF_CI_ProhibitedContent*, используемая участниками информационного обмена для уведомления Банка России о компьютерном инциденте – публикации на контролируемом ресурсе запрещенной законодательством Российской Федерации информации;
- форма представления данных *NTF_CI_SocialEngineering*, используемая участниками информационного обмена для уведомления Банка России о компьютерном инциденте – мошеннических действиях с использованием методов социальной инженерии;
- форма представления данных *NTF_CI_TrafficHijacking*, используемая участниками информационного обмена для уведомления Банка России о компьютерном инциденте – захвате сетевого трафика;
- форма представления данных *NTF_CI_MalwareCommandControl*, используемая участниками информационного обмена для уведомления Банка России о компьютерном инциденте – вовлечении контролируемого ресурса в инфраструктуру вирусного программного обеспечения;
- форма представления данных *NTF_CI_Spam*, используемая участниками информационного обмена для уведомления Банка России о компьютерном инциденте – рассылке спам-сообщений с контролируемого ресурса;
- форма представления данных *NTF_CI_UnauthorisedModification*, используемая участниками информационного обмена для уведомления Банка России о компьютерном инциденте – несанкционированном изменении информации;
- форма представления данных *NTF_CI_UnauthorisedAccess*, используемая участниками информационного обмена для уведомления Банка России о компьютерном инциденте – несанкционированном разглашении информации;
- форма представления данных *NTF_CI_SIM*, используемая участниками информационного обмена для уведомления Банка России о компьютерном инциденте – изменении (подмене) идентификатора мобильного абонента (*IMSI*), идентификатора мобильного оборудования (*IMEI*) или сим-карты.

7.3. ПРЕДСТАВЛЕНИЕ УЧАСТНИКАМИ ИНФОРМАЦИОННОГО ОБМЕНА ДАННЫХ О КОМПЬЮТЕРНЫХ АТАКАХ

Данные о компьютерных атаках направляются участниками информационного обмена в Банк России в соответствии с частью 2 статьи 9 Федерального закона № 187-ФЗ [2] и частями 4, 6 и 7 статьи 27 Федерального закона № 161 ФЗ [3] при выявлении критериев информирования о компьютерной атаке в соответствии с перечнем компьютерных атак, приведенным в разделе 7.1, а также в случаях, предусмотренных разделом 7.5 настоящего стандарта.

Информирование Банка России о компьютерных атаках осуществляется в формате сводного уведомления за отчетный период (период, за который осуществляется свод данных о компьютерных атаках). Свод данных включает в себя агрегацию данных по отдельным компьютерным атакам одного типа, в соответствии с перечнем компьютерных атак, приведенным в разделе 7.1, в единую форму представления данных. Агрегация данных осуществляется по полям формы представления данных.

При выявлении указанных критериев информирования участники информационного обмена направляют информацию о компьютерных атаках в отчетный период в соответствии со следующими сроками:

- свод данных о компьютерных атаках в случаях, если объектом вредоносной активности является ресурс, IP-адрес которого в соответствии с реестром адресно-номерных ресур-

сов принадлежит Российской Федерации, осуществляется за три календарных дня и направляется в течение 3 календарных дней, следующих за отчетным периодом;
- свод данных о компьютерных атаках в случаях, если объектом вредоносной активности является иной ресурс, осуществляется за 7 календарных дней и направляется в течение 7 календарных дней, следующих за отчетным периодом;
- свод данных о компьютерных атаках за другой период осуществляется по согласованию с ФинЦЕРТ Банка России.

Форма представления участниками информационного обмена данных о компьютерных атаках (*NTF_CA*) приведена в приложении 21 к настоящему стандарту.

В приложении 22 приведены следующие формы представления данных, которые являются предзаполненными вариантами формы *NTF_CA* и ориентированы на конкретные типы компьютерных атак в соответствии с перечнем компьютерных атак:
- форма представления данных *NTF_CA_DoS*, используемая участниками информационного обмена для уведомления Банка России о компьютерных атаках типа «Отказ в обслуживании»;
- форма представления данных *NTF_CA_ExploitAttempt*, используемая участниками информационного обмена для уведомления Банка России о компьютерных атаках – попытках эксплуатации уязвимостей;
- форма представления данных *NTF_CA_InfectionAttempt*, используемая участниками информационного обмена для уведомления Банка России о компьютерных атаках – попытках внедрения модулей вредоносного программного обеспечения;
- форма представления данных *NTF_CA_LoginAttempt*, используемая участниками информационного обмена для уведомления Банка России о компьютерных атаках – неуспешных попытках авторизации;
- форма представления данных *NTF_CA_Phishing*, используемая участниками информационного обмена для уведомления Банка России о компьютерных атаках – выявлении фишинговой рассылки или ресурса;
- форма представления данных *NTF_CA_SocialEngineering*, используемая участниками информационного обмена для уведомления Банка России о компьютерных атаках – мошеннических действиях с использованием методов социальной инженерии;
- форма представления данных *NTF_CA_Scanning*, используемая участниками информационного обмена для уведомления Банка России о компьютерных атаках – сетевом сканировании контролируемого ресурса.

7.4. ПРЕДСТАВЛЕНИЕ УЧАСТНИКАМИ ИНФОРМАЦИОННОГО ОБМЕНА ДАННЫХ О ВЫЯВЛЕННЫХ УЯЗВИМОСТЯХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Данные о выявленных уязвимостях информационной безопасности направляются участниками информационного обмена в Банк России в соответствии с частью 2 статьи 9 Федерального закона № 187-ФЗ [2], а также положениями Банка России № 757-П [7], № 683-П [5], № 719-П [6] при выявлении в результате выполнения процедур по контролю отсутствия известных (описанных) уязвимостей информационной безопасности или регулярного тестирования объектов информационной инфраструктуры на предмет проникновений и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры, предусмотренных положениями Банка России № 683-П [5], № 719-П [6], № 757-П [7], уязвимостей информационной безопасности в объектах информационной инфраструктуры, полученных от сторонней организации-поставщика по лицензионному договору или договору поставки, и информация о данной уязвимости информационной безопасности не размещена на официальном сайте организации-поставщика либо прикладном программном обеспечении, распространяемом участником информационного обмена сторонним организациям, а также в случаях, предусмотренных разделом 7.5 настоящего стандарта.

При выявлении указанных условий информирования участники информационного обмена направляют информацию о выявленных уязвимостях информационной безопасности в соответствии со следующими сроками:

- в течение 24 часов с момента самостоятельного выявления уязвимости информационной безопасности;
- в течение 3 дней с момента получения отчета сторонней организации, содержащего информацию об уязвимостях информационной безопасности объектов информационной инфраструктуры.

Форма представления участниками информационного обмена данных о выявленных уязвимостях информационной безопасности (*NTF_VLN*) приведена в приложении 23 к настоящему стандарту.

7.5. ЗАПРОС БАНКА РОССИИ К УЧАСТНИКАМ ИНФОРМАЦИОННОГО ОБМЕНА В ЦЕЛЯХ ПОЛУЧЕНИЯ СВЕДЕНИЙ О ВЫЯВЛЕННОЙ КОМПЬЮТЕРНОЙ АТАКЕ ИЛИ УЯЗВИМОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Запрос к участнику информационного обмена в целях получения сведений о выявленной компьютерной атаке или уязвимости информационной безопасности при необходимости направляется Банком России при получении сведений о компьютерной атаке или выявленной уязвимости информационной безопасности в объекте информатизации участника информационного обмена с целью получения подтверждения факта компьютерной атаки или уязвимости информационной безопасности в соответствии с частью 2 статьи 9 Федерального закона № 187-ФЗ [2], пунктом 4 Порядка, утвержденного приказом ФСБ России № 282.

При получении запроса в целях получения сведений о выявленной компьютерной атаке или уязвимости информационной безопасности участники информационного обмена направляют следующие формы представления данных в соответствии с указанными сроками:

- форму представления данных *NTF_CI* в течение 3 часов в случае выявления на основании сведений из запроса Банка России компьютерного инцидента, связанного с функционированием значимого объекта критической информационной инфраструктуры;
- форму представления данных *NTF_CI* в течение 24 часов в случае выявления на основании сведений из запроса Банка России компьютерного инцидента, не связанного с функционированием значимого объекта критической информационной инфраструктуры;
- форму представления данных *NTF_CA* в течение 24 часов в случае выявления на основании сведений из запроса Банка России компьютерной атаки;
- форму представления данных *NTF_VLN* в течение 24 часов в случае выявления на основании сведений из запроса Банка России уязвимости информационной безопасности в объекте информатизации;
- форму *RESP_IEP_Detect* в течение 24 часов, в случае если на основании сведений из запроса Банка России не были выявлены компьютерные инциденты, компьютерные атаки или уязвимости информационной безопасности.

Форма запроса Банка России, направляемого участнику информационного обмена в целях получения сведений о выявленной компьютерной атаке или уязвимости информационной безопасности (*REQ_IEP_Detect*), а также форма для представления ответа Банку России, содержащего информацию о невыявлении компьютерной атаки или уязвимости информационной безопасности (*RESP_IEP_Detect*), направляемая в случае, предусмотренном абзацем 7 раздела 7.5 настоящего стандарта, приведены в приложении 24 к настоящему стандарту.

7.6. ЗАПРОС БАНКА РОССИИ В ЦЕЛЯХ ПОЛУЧЕНИЯ СВЕДЕНИЙ О ПРИНАДЛЕЖНОСТИ УЧАСТНИКУ ИНФОРМАЦИОННОГО ОБМЕНА РЕСУРСА В СЕТИ ИНТЕРНЕТ

Запрос Банка России к участнику информационного обмена в целях получения сведений о принадлежности ему ресурса в сети Интернет при необходимости направляется Банком России при получении информации о ресурсе в сети Интернет, содержащем вредоносный код,

фишинговую или запрещенную законодательством РФ информацию, в рамках уведомления о компьютерных инцидентах или атаках с целью получения подтверждения принадлежности выявленного ресурса в сети Интернет участнику информационного обмена в целях реализации Банком России положений статьи 6.2 Федерального закона № 86-ФЗ [1].

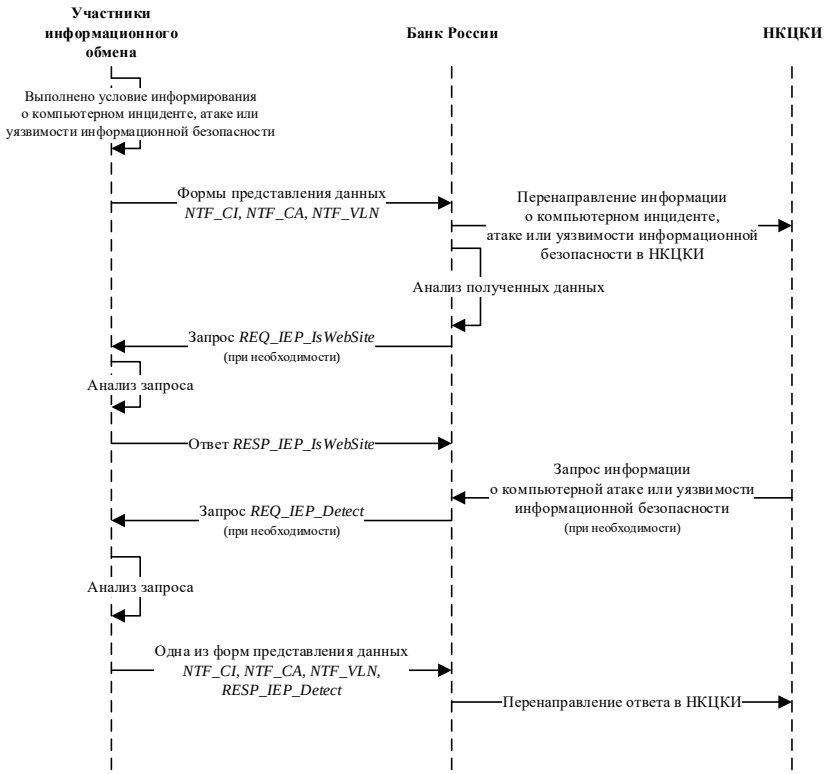
При получении запроса в целях получения сведений о принадлежности выявленного ресурса в сети Интернет участники информационного обмена направляют информацию в течение 24 часов с момента получения запроса Банка России.

Форма запроса Банка России, направляемого участнику информационного обмена в целях получения сведений о принадлежности участнику информационного обмена ресурса в сети Интернет (*REQ_IEP_IsWebSite*), а также форма для представления ответа Банку России, содержащего информацию о принадлежности участнику информационного обмена выявленного ресурса в сети Интернет (*RESP_IEP_IsWebSite*), приведены в приложении 25 к настоящему стандарту.

7.7. СХЕМА ВЗАИМОДЕЙСТВИЯ БАНКА РОССИИ И УЧАСТНИКОВ ИНФОРМАЦИОННОГО ОБМЕНА ПРИ ВЫЯВЛЕНИИ КОМПЬЮТЕРНЫХ ИНЦИДЕНТОВ, КОМПЬЮТЕРНЫХ АТАК И УЯЗВИМОСТЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Схема взаимодействия Банка России и участников информационного обмена при выявлении компьютерных инцидентов, компьютерных атак и уязвимостей информационной безопасности представлена на рис. 5.

РИС. 5. СХЕМА ВЗАИМОДЕЙСТВИЯ БАНКА РОССИИ И УЧАСТНИКОВ ИНФОРМАЦИОННОГО ОБМЕНА ПРИ ВЫЯВЛЕНИИ КОМПЬЮТЕРНЫХ ИНЦИДЕНТОВ, КОМПЬЮТЕРНЫХ АТАК И УЯЗВИМОСТЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



8. ВЗАИМОДЕЙСТВИЕ УЧАСТНИКОВ ИНФОРМАЦИОННОГО ОБМЕНА И БАНКА РОССИИ В ЦЕЛЯХ ПРИОСТАНОВЛЕНИЯ/ОТМЕНЫ ПРИОСТАНОВЛЕНИЯ ОБМЕНА ЭЛЕКТРОННЫМИ СООБЩЕНИЯМИ ПРИ ВЫЯВЛЕНИИ ИНЦИДЕНТОВ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ОСУЩЕСТВЛЕНИИ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ С ИСПОЛЬЗОВАНИЕМ ССНП НА ОБЪЕКТАХ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ УЧАСТНИКОВ ИНФОРМАЦИОННОГО ОБМЕНА

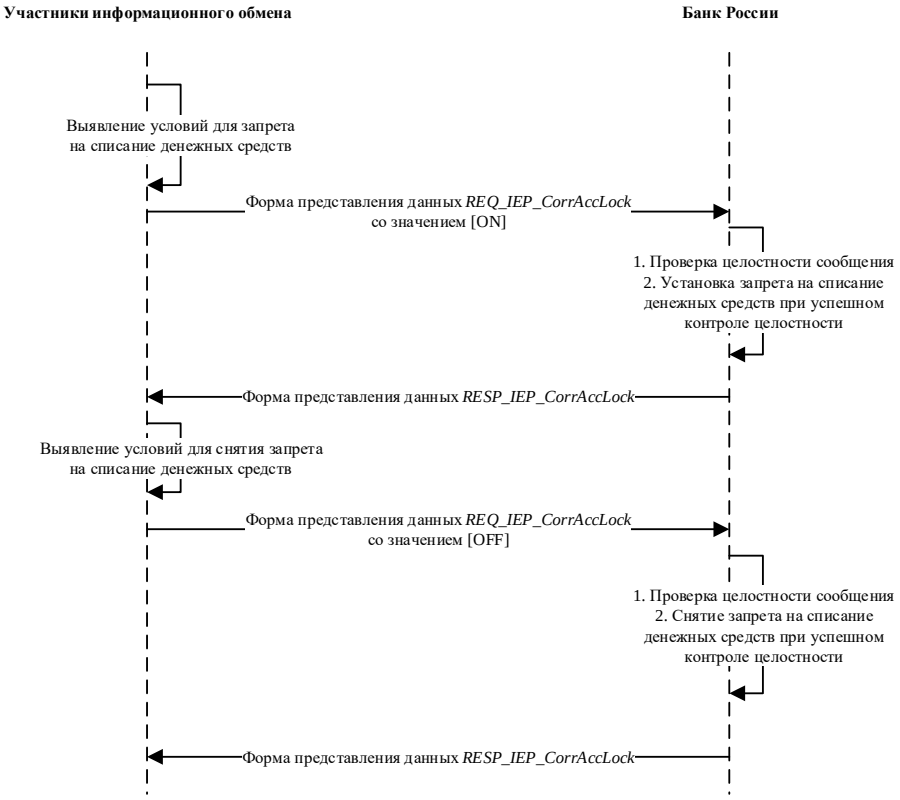
Запрос в Банк России о приостановлении/отмене приостановления обмена электронными сообщениями направляется участниками информационного обмена – участниками ССНП в Банк России в соответствии с пунктом 19 Положения Банка России от 25 июля 2022 года № 802-П «О требованиях к защите информации в платежной системе Банка России» (далее – Положение Банка России № 802-П) [8] при выявлении инцидентов защиты информации при осуществлении переводов денежных средств с использованием ССНП на объектах информационной инфраструктуры участников информационного обмена, которые привели или могут привести к осуществлению перевода денежных средств без согласия участника информационного обмена.

При выявлении указанных условий информирования участники информационного обмена направляют информацию о приостановлении/отмене приостановления обмена электронными сообщениями в соответствии пунктом 18 Положения Банка России № 802-П. Форма запроса участника информационного обмена, использующего ССНП для осуществления перевода денежных средств, направляемого в Банк России в целях приостановления/отмены приостановления обмена электронными сообщениями при выявлении инцидентов защиты информации при осуществлении переводов денежных средств с использованием ССНП на объектах информационной инфраструктуры участников информационного обмена (*REQ_IEP_CorrAccLock*), приведена в приложении 26 к настоящему стандарту.

При получении запроса от участника информационного обмена Банк России направляет уведомление о рассмотрении запроса в соответствии с пунктом 19.5 Положения Банка России № 802-П [8]. Форма для представления ответа участнику информационного обмена, содержащего информацию о рассмотрении запроса о приостановлении/отмене приостановления обмена электронными сообщениями (*RESP_IEP_CorrAccLock*), приведена в приложении 26 к настоящему стандарту.

Схема взаимодействия Банка России и участников информационного обмена при запросе на приостановление/отмену приостановления обмена электронными сообщениями при выявлении инцидентов защиты информации при осуществлении переводов денежных средств с использованием ССНП на объектах информационной инфраструктуры участников информационного обмена представлена на рис. 6.

РИС. 6. СХЕМА ВЗАИМОДЕЙСТВИЯ БАНКА РОССИИ И УЧАСТНИКОВ ИНФОРМАЦИОННОГО ОБМЕНА ПРИ ЗАПРОСЕ НА ПРИОСТАНОВЛЕНИЕ/ОТМЕНУ ПРИОСТАНОВЛЕНИЯ ОБМЕНА ЭЛЕКТРОННЫМИ СООБЩЕНИЯМИ ПРИ ВЫЯВЛЕНИИ ИНЦИДЕНТОВ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ОСУЩЕСТВЛЕНИИ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ НА ОБЪЕКТАХ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ УЧАСТНИКОВ ИНФОРМАЦИОННОГО ОБМЕНА



9. НАПРАВЛЕНИЕ УЧАСТНИКАМИ ИНФОРМАЦИОННОГО ОБМЕНА В БАНК РОССИИ ИНФОРМАЦИИ О ПЛАНИРУЕМЫХ МЕРОПРИЯТИЯХ ПО РАСКРЫТИЮ ИНФОРМАЦИИ О ВЫЯВЛЕННЫХ ИНЦИДЕНТАХ ЗАЩИТЫ ИНФОРМАЦИИ ИЛИ ИНЦИДЕНТАХ ОПЕРАЦИОННОЙ НАДЕЖНОСТИ

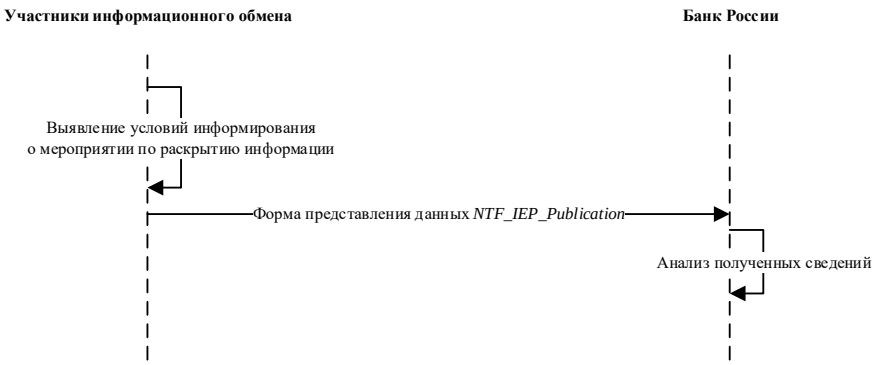
Данные о планируемых мероприятиях по раскрытию информации о выявленных инцидентах защиты информации или инцидентах операционной надежности направляются участниками информационного обмена в Банк России в соответствии с абзацем четвертым пункта 1.15 Положения Банка России № 757-П [7], абзацем девятым пункта 8 Положения Банка России № 683-П [5], абзацем третьим пункта 1.5 Положения Банка России № 719-П [6], абзацем третьим пункта 11 Положения Банка России № 787-П [9] и абзацем третьим пункта 1.15 Положения Банка России № 779-П [10], при наступлении следующего условия: участником информационного обмена планируются мероприятия, включая выпуск пресс-релизов и проведение пресс-конференций, размещение информации на официальных сайтах в сети Интернет, в отношении инцидентов защиты информации или инцидентов операционной надежности.

При выявлении указанного условия информирования участники информационного обмена направляют информацию о планируемых мероприятиях по раскрытию информации о выявленных инцидентах защиты информации или инцидентов операционной надежности в соответствии со сроками, установленными абзацем четвертым пункта 1.15 Положения Банка России № 757-П [7], абзацем девятым пункта 8 Положения Банка России № 683-П [5], абзацем третьим пункта 1.5 Положения Банка России № 719-П [6], абзацем третьим пункта 11 Положения Банка России № 787-П [9] и абзацем третьим пункта 1.15 Положения Банка России № 779-П [10].

Форма направления участниками информационного обмена в Банк России информации о планируемых мероприятиях по раскрытию информации о выявленных инцидентах защиты информации или инцидентах операционной надежности (*NTF_IEP_Publication*), приведена в приложении 27 к настоящему стандарту.

Схема взаимодействия Банка России и участников информационного обмена при направлении информации о планируемых мероприятиях по раскрытию информации о выявленных инцидентах защиты информации или инцидентах операционной надежности представлена на рис. 7.

РИС. 7. СХЕМА ВЗАИМОДЕЙСТВИЯ БАНКА РОССИИ И УЧАСТНИКОВ ИНФОРМАЦИОННОГО ОБМЕНА ПРИ НАПРАВЛЕНИИ ИНФОРМАЦИИ О ПЛАНИРУЕМЫХ МЕРОПРИЯТИЯХ ПО РАСКРЫТИЮ ИНФОРМАЦИИ О ВЫЯВЛЕННЫХ ИНЦИДЕНТАХ ЗАЩИТЫ ИНФОРМАЦИИ ИЛИ ИНЦИДЕНТАХ ОПЕРАЦИОННОЙ НАДЕЖНОСТИ



ПРИЛОЖЕНИЯ

ПРИЛОЖЕНИЕ 1. ФОРМА ПРЕДСТАВЛЕНИЯ ДАННЫХ NTF_OWC_SNPS – ФОРМА ПРЕДСТАВЛЕНИЯ ДАННЫХ УЧАСТНИКАМИ ИНФОРМАЦИОННОГО ОБМЕНА – ОПЕРАТОРАМИ ПО ПЕРЕВОДУ ДЕНЕЖНЫХ СРЕДСТВ, ОПЕРАТОРАМИ ПЛАТЕЖНЫХ СИСТЕМ, ОПЕРАТОРАМИ УСЛУГ ПЛАТЕЖНОЙ ИНФРАСТРУКТУРЫ ОБО ВСЕХ СЛУЧАЯХ И (ИЛИ) ПОПЫТКАХ ОСУЩЕСТВЛЕНИЯ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ БЕЗ СОГЛАСИЯ КЛИЕНТА

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип уведомления	Тип уведомления	О	-	[NTF_OWC_SNPS]	Предзаполненное поле
2	Информация об идентификаторах плательщика (идентифицирующая плательщика)	ИНН	УО	Если плательщик – юридическое лицо, иначе при наличии	В соответствии с форматом ФНС России	Обязательно заполняется хотя бы одно из полей
3		Результат вычисления специального кода номера ДУЛ	УО	Если плательщик – физическое лицо	Результат вычисления хеш-функции SHA-256	
4		Результат вычисления специального кода номера СНИЛС	УО	Если плательщик – физическое лицо, при наличии	Результат вычисления хеш-функции SHA-256	-
5		Абонентский номер подвижной радиотелефонной связи	УО	Если плательщик – физическое лицо, иначе при наличии	В соответствии с международной системой и планом нумерации	Абонентский номер подвижной радиотелефонной связи плательщика, подтвержденный в соответствии с п. 5.2.1 Положения № 683-П
6	Критерии легитимности операции без согласия, характеризующие плательщика	Критерии легитимности операции без согласия, характеризующие плательщика	УО	Если плательщик соответствует хотя бы одному из критериев легитимности	Из классификатора «Критерии легитимности (признаки осуществления перевода денежных средств без согласия клиента) операции без согласия», приведенного в приложении 28	Выбираются все критерии легитимности операции без согласия, характеризующие плательщика
7	Информация о средстве платежа плательщика	Тип средства платежа плательщика	О	-	Выбор одного значения из списка: [Наличные] [Банковский счет] [Платежная карта] [Абонентский номер подвижной радиотелефонной связи] [Электронный кошелек]	-
8		Номер банковского счета	УО	Поле «Тип средства платежа» = [Банковский счет]	В соответствии с форматом, определенным Положением Банка России № 579-П	-
9		БИК оператора по переводу денежных средств			В соответствии с форматом, определенным Положением Банка России № 732-П	-
10		Номер платежной карты	УО	Поле «Тип средства платежа» = [Платежная карта]	В соответствии с форматом ISO/IEC 7812	-

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
11		Абонентский номер подвижной радиотелефонной связи	УО	Поле «Тип средства платежа» = [Абонентский номер подвижной радиотелефонной связи]	В соответствии с международной системой и планом нумерации	-
12		Идентификатор электронного кошелька	УО	Поле «Тип средства платежа» = [Электронный кошелек]	В соответствии с форматом идентификаторов электронных кошельков, определенных оператором электронных денежных средств	-
13		ИНН оператора электронных денежных средств, выпустившего электронный кошелек			В соответствии с форматом, утвержденным ФНС России	
14	Информация о способе проведения операции	Технология осуществления перевода денежных средств	О	-	Выбор одного значения из списка: [INT] [CARD] [WALLET] [PS BR] [SPFS] [SWIFT] [SBP] [MONEY] Перечень зависит от поля «Тип средства платежа плательщика»	[INT] – внутренний перевод [CARD] – карточные платежные системы [WALLET] – платежные системы без открытия счета [PS_BR] – межбанковские переводы с использованием ПС БР [SPFS] – межбанковские переводы с использованием СПФС [SWIFT] – межбанковские переводы с использованием SWIFT [SBP] – межбанковские переводы с использованием СБП [MONEY] – быстрые денежные переводы без открытия счета
15		Платежная система	УО	Поле «Технология осуществления перевода денежных средств» = [CARD], [WALLET], [MONEY]	ИНН, в соответствии с форматом ФНС России, или [Иное]	В случае наличия ИНН у оператора платежной системы или оператора электронных денежных средств указывается ИНН, иначе значение [Иное]

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
16		Тип операции	О	-	«Выбор одного значения из списка: [FUND] [WITHDRAW] [TRANSFER] [CROSS] [PURCHASE] [CHARGEBACK] [B2B] [B2C] [C2B] [C2C] [C2G] Перечень зависит от полей «Тип средства платежа плательщика» и «Платежная система»	[FUND] – внесение наличных денежных средств [WITHDRAW] – снятие наличных денежных средств [TRANSFER] – перевод денежных средств между однотипными средствами платежа [CROSS] – перевод денежных средств с конвертацией между разнотипными средствами платежа [PURCHASE] – покупка [CHARGEBACK] – возврат [B2B] – B2B-операции в СБП [B2C] – B2C-операции в СБП [C2B] – C2B-операции в СБП [C2C] – C2C-операции в СБП [C2G] – C2G-операции в СБП
17	Информация о средстве платежа получателя	Тип средства платежа получателя средств	УО	Поле «Тип операции» = [PURCHASE], [C2B], [B2B] заполняется при наличии	«Выбор одного значения из списка: [Наличные] [Банковский счет] [Платежная карта] [Абонентский номер подвижной радиотелефонной связи] [Электронный кошелек] Перечень зависит от полей «Платежная система» и «Тип операции»	-
18		Номер банковского счета	УО	Поле «Тип средства платежа» = [Банковский счет]	В соответствии с форматом, определенным Положением Банка России № 579-П	-
19		БИК оператора по переводу денежных средств			В соответствии с форматом, определенным Положением Банка России № 732-П	-
20		Номер платежной карты	УО	Поле «Тип средства платежа» = [Платежная карта]	В соответствии с форматом ISO/IEC 7812	-
21		Абонентский номер подвижной радиотелефонной связи	УО	Поле «Тип средства платежа» = [Абонентский номер подвижной радиотелефонной связи]	В соответствии с международной системой и планом нумерации	-

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
22		Идентификатор электронного кошелька	УО	Поле «Тип средства платежа» = [Электронный кошелек]	В соответствии с форматом идентификаторов электронных кошельков, определенных оператором электронных денежных средств	-
23		ИНН оператора электронных денежных средств, выпустившего электронный кошелек			В соответствии с форматом, утвержденным ФНС России	-
24	Информация об идентификаторах получателя средств (идентифицирующая получателя средств)	ИНН	УО	Поле «Технология осуществления перевода денежных средств» = [INT]	В соответствии с форматом ФНС России	Обязательно заполняется хотя бы одно из полей
25		Результат вычисления специального кода номера ДУЛ			Результат вычисления хеш-функции SHA-256	
26		Результат вычисления специального кода номера СНИЛС			Результат вычисления хеш-функции SHA-256	При наличии
27		Абонентский номер подвижной радиотелефонной связи			В соответствии с международной системой и планом нумерации	Абонентский номер подвижной радиотелефонной связи получателя средств, подтвержденный в соответствии с п. 5.2.1 Положения № 683-П
28	Критерии легитимности операции без согласия, характеризующие получателя средств	Критерии легитимности операции без согласия, характеризующие получателя средств	УО	Поле «Технология осуществления перевода денежных средств» = [INT], и получатель средств соответствует хотя бы одному из критериев легитимности	Из классификатора «Критерии легитимности (признаки осуществления перевода денежных средств без согласия клиента) операции без согласия», приведенного в приложении 28	Выбираются все критерии легитимности операции без согласия, характеризующие получателя средств
29	Информация, устанавливающая операцию по переводу денежных средств	Дата и время операции	О	-	В соответствии с RFC 3339	По московскому времени [UTC +03:00]
30		Сумма операции	О	-	Сумма без учета комиссии банка с точностью до двух знаков после запятой	-
31		Валюта операции	О	-	Из Общероссийского классификатора валют	-
32		Сумма операции в рублях по внутреннему курсу	УО	Поле «Валюта операции» ≠ [RUB]	Сумма с точностью до двух знаков после запятой	-
33		Назначение платежа	Н	-	Текстовое поле	-
34		БИК оператора по переводу денежных средств, обслуживающего получателя средств	О	-	В соответствии с форматом, определенным Положением Банка России № 732-П	-

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
35		Идентификатор оператора по переводу денежных средств, обслуживающего плательщика, при использовании СПФС или SWIFT	УО	Поле «Технология осуществления перевода денежных средств» = [SPFS], [SWIFT]	В соответствии с форматом SWIFT	SWIFT-code плательщика
36		Идентификатор оператора по переводу денежных средств, обслуживающего получателя средств, при использовании СПФС или SWIFT			В соответствии с форматом SWIFT	SWIFT-code получателя средств
37		Идентификатор операции SWIFT (номер операции)			В соответствии с форматом SWIFT	-
38		Идентификатор торгово-сервисного предприятия	УО	При операции в адрес торгово-сервисного предприятия	В соответствии с форматом, утвержденным платежной системой	MerchantID
39		ИНН торгово-сервисного предприятия	УО	При операции в адрес торгово-сервисного предприятия, при наличии	В соответствии с форматом, утвержденным ФНС России	-
40		Ссылочный номер операции (транзакции)	УО	Поле «Технология осуществления перевода денежных средств» = [CARD]	В соответствии с форматом, утвержденным платежной системой	Retrieval Reference Number (RRN)
41		Код ответа операции (транзакции)			[Одобрена] [Отклонена]	Response Code
42		Код причины возврата			В соответствии с форматом, утвержденным платежной системой	Reason Code
43		BIN оператора по переводу денежных средств – эквайрера			В соответствии с форматом, утвержденным платежной системой	-
44		Код, отражающий основной вид деятельности торгово-сервисного предприятия	УО	Поле «Технология осуществления перевода денежных средств» = [CARD], и заполнение данного поля в авторизационных сообщениях предусмотрено стандартами ПС	В соответствии с форматом, утвержденным платежной системой	MCC
45		Значение токена при токенизированной операции	УО	Поле «Технология осуществления перевода денежных средств» = [CARD], и проводилась операция с токенизированной картой	В соответствии с форматом, утвержденным платежной системой	Token Number
46		Идентификатор СБП оператора по переводу денежных средств, обслуживающего получателя средств	УО	Поле «Технология осуществления перевода денежных средств» = [SBP]	В соответствии со стандартами ОПКЦ СБП	MemberID
47		Идентификатор операции СБП (номер операции)	УО	Поле «Технология осуществления перевода денежных средств» = [SBP]	В соответствии со стандартами ОПКЦ СБП	TR ID

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
48		Идентификатор платежной ссылки СБП	УО	Поле «Технология осуществления перевода денежных средств» = [SBP] и «Тип операции» = [B2B], [C2B], [C2G], и операция выполнялась с использованием платежной ссылки	В соответствии со стандартами ОПКЦ СБП	QRC_ID
49	Информация об операции без согласия	Условие уведомления об операции без согласия	О	-	Выбор одного значения из списка: [Client OWC] [Client Attempt] [Participant] [DB] [IND] [REQ]	[Client OWC] – уведомление от клиента об ОБС [Client Attempt] – уведомление от клиента о попытке ОБС [Participant] – уведомление от участника ПС [DB] – наличие в БД об ОБС [IND] – выявление признаков ОД-2525 [REQ] – получение информации о совершенных противоправных действиях в рамках запроса Банка России и классификация операции по переводу денежных средств как операции без согласия клиента
50		Идентификатор (-ы) запроса (-ов) Банка России в целях получения данных об операции без согласия на основании сведений о совершенных противоправных действиях от федерального органа исполнительной власти в сфере внутренних дел	УО	Поле «Условие уведомления об операции без согласия» = [REQ]	В соответствии с форматом АСОИ ФинЦЕРТ. При указании нескольких идентификаторов, необходимо их перечислять через «;»	Идентификатор (-ы) запроса (-ов) Банка России в целях получения данных об операции без согласия на основании сведений о совершенных противоправных действиях от федерального органа исполнительной власти в сфере внутренних дел, в рамках которого операция по переводу денежных средств была классифицирована как операция без согласия клиента
51		Дата и время регистрации уведомления об операции без согласия или выявления попытки операции без согласия	О	-	В соответствии с RFC 3339	По московскому времени [UTC +03:00]

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
52		Критерии легитимности операции без согласия, характеризующие операцию	УО	Если операция соответствует хотя бы одному из критериев легитимности	Из классификатора «Критерии легитимности (признаки осуществления перевода денежных средств без согласия клиента) операции без согласия», приведенного в приложении 28	Выбираются все критерии легитимности операции без согласия, характеризующие операцию
53		Сумма ущерба	О	-	Сумма операции с учетом комиссии банка с точностью до двух знаков после запятой	Указывается сумма фактических потерь клиента
54		Использование ЕБС для идентификации клиента	УО	Если идентификация клиента проводилась с использованием ЕБС	[Да]	-
55	Информация, используемая для идентификации устройств	Способ проведения операции	О	-	Выбор одного значения из списка: [ATM] [BRANCH] [DBO]. [MB] [DBO]. [WEB] [DBO]. [TC] [ECOM] [POS] [SST]	[ATM] – с использованием банкомата [BRANCH] – в отделении кредитной организации [DBO]. [MB] – с использованием мобильного банка [DBO]. [WEB] – с использованием банк-клиента (тонкий клиент) [DBO]. [TC] – с использованием банк-клиента (толстый клиент) [ECOM] – с использованием средств электронной комерции [POS] – с использованием POS терминала [SST] – с использованием терминала самообслуживания
56		Идентификатор устройства	УО	Поле «Способ проведения операции» = [ATM], [POS] или [SST]	Текстовое поле	Уникальный идентификатор устройства, с которого осуществлялась операция
57		Уникальный числовой идентификатор устройства в сети Интернет	УО	Поле «Способ проведения операции» = [DBO]. [MB], [DBO]. [WEB], [DBO]. [TC]	В соответствии с форматом RFC 791 или RFC 2460	IP-адрес устройства
58		Сетевой адрес компьютера и (или) коммуникационного устройства (маршрутизатора)	Н	-	В соответствии с форматом IEEE	MAC-адрес устройства
59		Международный идентификатор абонента (индивидуальный номер абонента – физического лица)	Н	-	В соответствии с форматом ITU-T E. 118	Номер сим-карты (ICCID)

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
60		Международный идентификатор пользовательского оборудования (оконечного оборудования) абонента – физического лица	Н	-	В соответствии с форматом ITU-T E. 212	IMSI устройства
61		Цифровой отпечаток устройства	Н	-	Цифровой отпечаток устройства, собранный в соответствии с рекомендациями Банка России	-
62		Фишинговый URL	Н	-	В соответствии с форматом RFC 3986	Заполняется в случае инициации транзакции с фишингового сайта
63	Обращение плательщика в правоохранительные органы	Обращение в правоохранительные органы	Н	-	[Совершено]	-
64		Дата внесения в книгу учета сообщений о преступлениях	УО	«Обращение в правоохранительные органы» = [Совершено], заполняется как минимум один из блоков	В соответствии с RFC 3339	По московскому времени [UTC +03:00]
65		Порядковый номер в книге учета сообщений о преступлениях			В соответствии с форматом, установленным МВД России	-
66		Дата заведения уголовного дела	УО		В соответствии с RFC 3339	По московскому времени [UTC +03:00]
67		Номер уголовного дела			В соответствии с форматом, установленным МВД России	-
68	Необходимость привлечения ФинЦЕРТ	Необходимость привлечения ФинЦЕРТ для проведения расследования цепочки вывода денежных средств	УО	При необходимости	[Да]	-

ПРИЛОЖЕНИЕ 2. ФОРМА ПРЕДСТАВЛЕНИЯ ДАННЫХ NTF_OWC_OEP – ФОРМА ПРЕДСТАВЛЕНИЯ УЧАСТНИКАМИ ИНФОРМАЦИОННОГО ОБМЕНА – ОПЕРАТОРАМИ ЭЛЕКТРОННЫХ ПЛАТФОРМ ДАННЫХ ОБО ВСЕХ СЛУЧАЯХ И (ИЛИ) ПОПЫТКАХ ОСУЩЕСТВЛЕНИЯ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ БЕЗ СОГЛАСИЯ КЛИЕНТА, ВКЛЮЧАЮЩИХ ИНФОРМАЦИЮ ОБ ОПЕРАЦИЯХ ПО НОМИНАЛЬНОМУ СЧЕТУ БЕЗ СОГЛАСИЯ КЛИЕНТА-БЕНЕФИЦИАРА

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип уведомления	Тип уведомления	О	-	[NTF_OWC_OEP]	Предзаполненное поле
2	Условие уведомления об операции без согласия	Условие уведомления об операции без согласия	О	-	Выбор одного значения из списка: [Client OWC] [Client Attempt] [DB] [UAA]	[Client OWC] – уведомление от клиента об ОБС [Client Attempt] – уведомление от клиента о попытке ОБС [UAA] – выявление несанкционированного доступа к объектам информационной инфраструктуры [DB] – наличие в БД об ОБС
3	Информация об идентификаторах клиента-бенефициара	ИНН	УО	Если плательщик – юридическое лицо, иначе при наличии	В соответствии с форматом ФНС России	Обязательно заполняется хотя бы одно из полей
4		Результат вычисления специального кода номера ДУЛ	УО	Если плательщик – физическое лицо	Результат вычисления хеш-функции SHA-256	
5		Результат вычисления специального кода номера СНИЛС	УО	Если плательщик – физическое лицо, при наличии	Результат вычисления хеш-функции SHA-256	-
6	Информация об идентификаторах ОЭП, по номинальному счету которого совершена операция без согласия клиента-бенефициара	Номер номинального счета	О	-	В соответствии с форматом, определенным Положением Банка России № 579-П	-
7		Наименование оператора по переводу денежных средств, в котором открыт номинальный счет	УО	Обязательно заполняется одно из полей	Из перечня, формируемого на основании официального справочника операторов по переводу денежных средств	-
8		БИК оператора по переводу денежных средств, в котором открыт номинальный счет			В соответствии с форматом, определенным Положением Банка России № 732-П	-
9	Информация об идентификаторах получателя средств в рамках операции, совершенной по номинальному счету без согласия клиента-бенефициара	Номер банковского счета	О	-	В соответствии с форматом, определенным Положением Банка России № 579-П	-
10		Наименование оператора по переводу денежных средств, в котором открыт банковский счет	УО	Обязательно заполняется одно из полей	Из перечня, формируемого на основании официального справочника операторов по переводу денежных средств	-

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
11		БИК оператора по переводу денежных средств, в котором открыт банковский счет			В соответствии с форматом, определенным Положением Банка России № 732-П	-
12	Информация об операции, совершенной по номинальному счету без согласия клиента-бенефициара	Дата и время операции	О	-	В соответствии с RFC 3339	По московскому времени [UTC +03:00]
13		Сумма операции	О	-	Сумма без учета комиссии банка с точностью до двух знаков после запятой	-
14		Валюта операции	О	-	Из Общероссийского классификатора валют	-
15		Сумма операции в рублях по внутреннему курсу	УО	Поле «Валюта операции» ≠ [RUB]	Сумма с точностью до двух знаков после запятой	-
16	Информация об операции без согласия	Дата и время регистрации уведомления об операции без согласия или выявления попытки операции без согласия	УО	Поле «Условие уведомления об операции без согласия» = [Client OWC], [Client Attempt]	В соответствии с RFC 3339	По московскому времени [UTC +03:00]
17		Критерии легитимности операции без согласия	О	-	Из классификатора «Критерии легитимности операции без согласия», приведенного в приложении 28	Выбираются все критерии легитимности, характеризующие операцию без согласия или плательщика
18		Сумма ущерба	О	-	Сумма операции с учетом комиссии банка с точностью до двух знаков после запятой	Указывается сумма фактических потерь клиента
19		Уникальный числовой идентификатор устройства в сети Интернет	Н	-	В соответствии с форматом RFC 791 или RFC 2460	IP-адрес устройства
20		Сетевой адрес компьютера и (или) коммуникационного устройства (маршрутизатора)	Н	-	В соответствии с форматом IEEE	MAC-адрес устройства
21		Международный идентификатор абонента (индивидуальный номер абонента – физического лица)	Н	-	В соответствии с форматом ITU-T E. 118	Номер сим-карты (ICCID)
22		Международный идентификатор пользовательского оборудования (оконечного оборудования) абонента – физического лица	Н	-	В соответствии с форматом ITU-T E. 212	IMSI устройства
23		Цифровой отпечаток устройства	Н	-	Цифровой отпечаток устройства, собранный в соответствии с рекомендациями Банка России	-

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
24	Обращение плательщика в правоохранительные органы	Обращение в правоохранительные органы	Н	-	[Совершено]	-
25		Дата внесения в книгу учета сообщений о преступлениях	УО	«Обращение в правоохранительные органы» = [Совершено]	В соответствии с RFC 3339	По московскому времени [UTC +03:00]
26		Порядковый номер в книге учета сообщений о преступлениях			В соответствии с форматом, установленным МВД России	-
27		Дата заведения уголовного дела			В соответствии с RFC 3339	По московскому времени [UTC +03:00]
28		Номер уголовного дела			В соответствии с форматом, установленным МВД России	-
29	Необходимость привлечения ФинЦЕРТ	Необходимость привлечения ФинЦЕРТ для проведения расследования цепочки вывода денежных средств	УО	При необходимости	[Да]	-

ПРИЛОЖЕНИЕ 3. ФОРМА ПРЕДСТАВЛЕНИЯ ДАННЫХ NTF_OWC_OFP – ФОРМА ПРЕДСТАВЛЕНИЯ УЧАСТНИКАМИ ИНФОРМАЦИОННОГО ОБМЕНА – ОПЕРАТОРАМИ ФИНАНСОВЫХ ПЛАТФОРМ ДАННЫХ ОБО ВСЕХ СЛУЧАЯХ И (ИЛИ) ПОПЫТКАХ ОСУЩЕСТВЛЕНИЯ ОПЕРАЦИЙ ПО ФИНАНСОВЫМ СДЕЛКАМ БЕЗ ВОЛЕИЗЪЯВЛЕНИЯ УЧАСТНИКА ФИНАНСОВОЙ ПЛАТФОРМЫ

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип уведомления	Тип уведомления	Тип уведомления	О	[NTF_OWC_OFP]	Предзаполненное поле
2	Условие уведомления об операции без волеизъявления	Условие уведомления об операции без волеизъявления	О	-	Выбор одного значения из списка: [Participant_accWithdrawal] [IND_accWithdrawal] [Participant_OWC] [IND_OWC]	[Participant_accWithdrawal] – уведомление от участника финансовой платформы о списании ДС со специального счета [IND_accWithdrawal] – самостоятельное выявление списания ДС со специального счета [Participant_OWC] – уведомление от участника финансовой платформы о сделке без волеизъявления [IND_OWC] – самостоятельное выявление сделки без волеизъявления
3	Информация, устанавливающая идентификаторы потребителя (идентифицирующая плательщика)	ИНН	О	Если ЮЛ, иначе при наличии	В соответствии с форматом ФНС России	Обязательно заполняется хотя бы одно из полей
4		Результат вычисления специального кода номера ДУЛ		Если ФЛ	Результат вычисления хеш-функции SHA-256	
5		Результат вычисления специального кода номера СНИЛС		Если ФЛ, при наличии	Результат вычисления хеш-функции SHA-256	
6	Данные о специальном счете ОФП, открытом в кредитной организации	Номер специального счета	УО	«Условие уведомления» = {«Participant_accWithdrawal», «IND_accWithdrawal»}	В соответствии с форматом, определенным Положением Банка России № 579-П	-
7		Наименование кредитной организации, обслуживающей ОФП	УО	Поле «Номер специального счета» заполнено. Обязательно заполняется одно из полей	Из перечня, формируемого на основании официального справочника операторов по переводу денежных средств	-
8		БИК кредитной организации, обслуживающей ОФП			В соответствии с форматом, определенным Положением Банка России № 732-П	-
9	Информация, устанавливающая идентификаторы получателя средств (идентифицирующая получателя средств)	ИНН	О	-	В соответствии с форматом ФНС России	-

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
10		Номер банковского счета	О	-	В соответствии с форматом, определенным Положением Банка России № 579-П	-
11		Наименование оператора по переводу денежных средств	О	-	Из перечня, формируемого на основании официального справочника операторов по переводу денежных средств	-
12		БИК оператора по переводу денежных средств	О	-	В соответствии с форматом, определенным Положением Банка России № 732-П	-
13	Информация, устанавливающая операцию (финансовую сделку) (блок заполняется отдельно для каждой операции без волеизъявления)	Вид финансовой сделки	УО	«Условие уведомления» = {«Participant_OWC», «IND_OWC»}	Выбор одного значения из списка: [Bank] [SIB] [PCB] [FI] [Other]	[Bank] – сделка по предоставлению банковских услуг [SIB] – сделка по предоставлению страховых услуг [PCB] – сделка по предоставлению услуг на рынке ценных бумаг [FI] – сделка с финансовыми инструментами [Other] – сделка по предоставлению иных предусмотренных правилами финансовой платформы услуг финансового характера, совершаемых между финансовыми организациями или эмитентами и потребителями финансовых услуг с использованием финансовой платформы, за исключением договоров банковского счета (вклада), заключаемых в связи с осуществлением потребителем финансовых услуг предпринимательской деятельности
14		Дата и время операции	О	-	В соответствии с RFC 3339	По московскому времени [UTC +03:00]
15		Сумма операции	О	-	Сумма с точностью до двух знаков после запятой	-
16		Валюта операции	О	-	Из Общероссийского классификатора валют	-
17		Сумма операции в рублях по внутреннему курсу	УО	Поле «Валюта операции» ≠ [RUB]	Сумма с точностью до двух знаков после запятой	-

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
18	Информация об операции без волеизъявления (блок заполняется для каждой операции из блока «Информация, устанавливающая операцию (финансовую сделку)»	Дата и время регистрации уведомления об операции без волеизъявления	УО	Поле «Условие уведомления об операции без согласия» = [Participant_accWithdrawal], [Participant_OWC]	В соответствии с RFC 3339	По московскому времени [UTC +03:00]
19		Критерии легитимности операции без волеизъявления	О	-	Из классификатора «Критерии легитимности операции без согласия», приведенного в приложении 28	Выбираются все критерии легитимности, характеризующие операцию без волеизъявления или потребителя
20		Сумма ущерба	О	-	Сумма с точностью до двух знаков после запятой	Указывается сумма фактических потерь клиента
21		Использование ЕБС для идентификации клиента	УО	Если идентификация клиента проводилась с использованием ЕБС	[Да]	-
22		Уникальный числовой идентификатор устройства в сети Интернет	Н	-	В соответствии с форматом RFC 791 или RFC 2460	IP-адрес устройства
23		Сетевой адрес компьютера и (или) коммуникационного устройства (маршрутизатора)	Н	-	В соответствии с форматом IEEE	MAC-адрес устройства
24		Международный идентификатор абонента (индивидуальный номер абонента – физического лица)	Н	-	В соответствии с форматом ITU-T E. 118	Номер сим-карты (ICCID)
25		Международный идентификатор пользовательского оборудования (оконечного оборудования) абонента – физического лица	Н	-	В соответствии с форматом ITU-T E. 212	IMSI устройства
26		Цифровой отпечаток устройства	Н	-	Цифровой отпечаток устройства, собранный в соответствии с рекомендациями Банка России	-
27		Фишинговый URL	Н	-	В соответствии с форматом RFC 3986	Заполняется в случае инициации транзакции с фишингового сайта

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
28	Обращение плательщика в правоохранительные органы	Обращение в правоохранительные органы	Н	-	[Совершено]	-
29		Дата внесения в книгу учета сообщений о преступлениях	УО	«Обращение в правоохранительные органы» = [Совершено]	В соответствии с RFC 3339	По московскому времени [UTC +03:00]
30		Порядковый номер в книге учета сообщений о преступлениях			В соответствии с форматом, установленным МВД России	-
31		Дата заведения уголовного дела			В соответствии с RFC 3339	По московскому времени [UTC +03:00]
32		Номер уголовного дела			В соответствии с форматом, установленным МВД России	-
33	Необходимость привлечения ФинЦЕРТ	Необходимость привлечения ФинЦЕРТ для проведения расследования цепочки вывода денежных средств	Н	-	[Да]	-

ПРИЛОЖЕНИЕ 4. ФОРМА ПРЕДСТАВЛЕНИЯ ДАННЫХ REQ_OWC_IDENTIFICATION – ФОРМА ЗАПРОСА БАНКА РОССИИ В ЦЕЛЯХ ИДЕНТИФИКАЦИИ ПОЛУЧАТЕЛЯ СРЕДСТВ ИЛИ ПЛАТЕЛЬЩИКА

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип запроса/ответа	Тип запроса/ответа	О	-	[REQ_OWC_ Identification]	Предзаполненное поле
2	Субъект запроса	Субъект запроса	О	-	[Получатель средств] [Плательщик]	-
3	Информация о средстве платежа получателя средств или плательщика	Тип средства платежа	О	-	Выбор одного значения из списка: [Наличные] [Банковский счет] [Платежная карта] [Абонентский номер подвижной радиотелефонной связи] [Электронный кошелек]	-
4		Номер банковского счета	УО	Поле «Тип средства платежа» = [Банковский счет]	В соответствии с форматом, определенным Положением Банка России № 579-П	-
5		БИК оператора по переводу денежных средств			В соответствии с форматом, определенным Положением Банка России № 732-П	-
6		Номер платежной карты	УО	Поле «Тип средства платежа» = [Платежная карта]	В соответствии с форматом ISO/IEC 7812	-
7		Абонентский номер подвижной радиотелефонной связи	УО	Поле «Тип средства платежа» = [Абонентский номер подвижной радиотелефонной связи]	В соответствии с международной системой и планом нумерации	-
8		Идентификатор электронного кошелька	УО	Поле «Тип средства платежа» = [Электронный кошелек]	В соответствии с форматом идентификаторов электронных кошельков, определенных оператором электронных денежных средств	-
9		ИНН оператора электронных денежных средств, выпустившего электронный кошелек			В соответствии с форматом, утвержденным ФНС России	-

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
10	Информация о способе проведения операции	Технология осуществления перевода денежных средств	О	-	Выбор одного значения из списка: [INT] [CARD] [WALLET] [PS BR] [SPFS] [SWIFT] [SBP] [MONEY] Перечень зависит от поля «Тип средства платежа плательщика»	[INT] – внутренний перевод [CARD] – карточные платежные системы [WALLET] – платежные системы без открытия счета [PS_BR] – межбанковские переводы с использованием ПС БР [SPFS] – межбанковские переводы с использованием СПФС [SWIFT] – межбанковские переводы с использованием SWIFT [SBP] – межбанковские переводы с использованием СБП [MONEY] – быстрые денежные переводы без открытия счета
11		Платежная система	УО	Поле «Технология осуществления перевода денежных средств» = [CARD], [WALLET], [MONEY]	ИНН, в соответствии с форматом ФНС России, или [Иное]	В случае наличия ИНН у оператора платежной системы или оператора электронных денежных средств указывается ИНН, иначе значение [Иное]
12		Тип операции	О	-	Выбор одного значения из списка: [FUND] [WITHDRAW] [TRANSFER] [CROSS] [PURCHASE] [CHARGEBACK] [B2B] [B2C] [C2B] [C2C] [C2G] Перечень зависит от полей «Тип средства платежа плательщика» и «Платежная система»	[FUND] – внесение наличных денежных средств [WITHDRAW] – снятие наличных денежных средств [TRANSFER] – перевод денежных средств между однотипными средствами платежа [CROSS] – перевод денежных средств с конвертацией между разнотипными средствами платежа [PURCHASE] – покупка [CHARGEBACK] – возврат [B2B] – B2B-операции в СБП [B2C] – B2C-операции в СБП [C2B] – C2B-операции в СБП [C2C] – C2C-операции в СБП [C2G] – C2G-операции в СБП

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
13	Информация, устанавливающая операцию по переводу денежных средств	Дата и время операции	О	-	В соответствии с RFC 3339	По московскому времени [UTC +03:00]
14		Сумма операции	О	-	Сумма без учета комиссии банка с точностью до двух знаков после запятой	-
15		Валюта операции	О	-	Из Общероссийского классификатора валют	-
16		Идентификатор оператора по переводу денежных средств, обслуживающего плательщика, при использовании СПФС или SWIFT	УО	Поле «Технология осуществления перевода денежных средств» = [SPFS], [SWIFT]	В соответствии с форматом SWIFT	SWIFT-code плательщика
17		Идентификатор оператора по переводу денежных средств, обслуживающего получателя средств, при использовании СПФС или SWIFT			В соответствии с форматом SWIFT	SWIFT-code получателя средств
18		Идентификатор операции SWIFT (номер операции)			В соответствии с форматом SWIFT	-
19		Идентификатор торгово-сервисного предприятия	УО	При операции в адрес торгово-сервисного предприятия	В соответствии с форматом, утвержденным платежной системой	MerchantID
20		ИНН торгово-сервисного предприятия	УО	При операции в адрес торгово-сервисного предприятия, при наличии	В соответствии с форматом, утвержденным ФНС России	-
21		Ссылочный номер операции (транзакции)	УО	Поле «Технология осуществления перевода денежных средств» = [CARD]	В соответствии с форматом, утвержденным платежной системой	Retrieval Reference Number (RRN)
22		Код ответа операции (транзакции)			[Одобрена] [Отклонена]	Response Code
23		Код причины возврата			В соответствии с форматом, утвержденным платежной системой	Reason Code
24		BIN оператора по переводу денежных средств – эквайрера			В соответствии с форматом, утвержденным платежной системой	-
25		Код, отражающий основной вид деятельности торгово-сервисного предприятия	УО	Поле «Технология осуществления перевода денежных средств» = [CARD], и заполнение данного поля в авторизационных сообщениях предусмотрено стандартами ПС	В соответствии с форматом, утвержденным платежной системой	MCC

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
26		Значение токена при токенизированной операции	УО	Поле «Технология осуществления перевода денежных средств» = [CARD], и проводилась операция с токенизированной картой	В соответствии с форматом, утвержденным платежной системой	Token Number
27		Идентификатор СБП оператора по переводу денежных средств, обслуживающего получателя средств	УО	Поле «Технология осуществления перевода денежных средств» = [SBP]	В соответствии со стандартами ОПКЦ СБП	MemberID
28		Идентификатор операции СБП (номер операции)	УО	Поле «Технология осуществления перевода денежных средств» = [SBP]	В соответствии со стандартами ОПКЦ СБП	TR ID
29		Идентификатор платежной ссылки СБП	УО	Поле «Технология осуществления перевода денежных средств» = [SBP] и «Тип операции» = [B2B], [C2B], [C2G], и операция выполнялась с использованием платежной ссылки	В соответствии со стандартами ОПКЦ СБП	QRC_ID
30	Критерии легитимности операции без согласия	Критерии легитимности операции без согласия	УО	При наличии	Из классификатора «Критерии легитимности (признаки осуществления перевода денежных средств без согласия клиента) операции без согласия», приведенного в приложении 28	-
31	Необходимость приостановления зачисления денежных средств	Необходимость приостановления зачисления денежных средств	УО	При необходимости осуществления приостановления зачисления денежных средств или увеличения остатка электронных денежных средств получателя средств	[Да]	-

Форма представления данных RESP_OWC_Identification – Форма представления ответа на запрос Банка России в целях идентификации получателя средств или плательщика

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип запроса/ответа	Тип запроса/ответа	О	-	[RESP_OWC_ Identification]	Предзаполненное поле
2	Статус	Статус	О	-	[Клиент и операция найдены] [Клиент не найден] [Операция не найдена] [P2P-операция] [Необходимо дополнительное время для рассмотрения]	-

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
3	Информация об идентификаторах получателя средств или плательщика	ИНН	УО	«Статус» = [Клиент и операция найдены] и ЮЛ, иначе при наличии	В соответствии с форматом ФНС России	Обязательно заполняется хотя бы одно из полей
4		Результат вычисления специального кода номера ДУЛ		«Статус» = [Клиент и операция найдены] и ФЛ	Результат вычисления хеш-функции SHA-256	
5		Результат вычисления специального кода номера СНИЛС		«Статус» = [Клиент и операция найдены] и ФЛ, при наличии	Результат вычисления хеш-функции SHA-256	При наличии
6		Абонентский номер подвижной радиотелефонной связи		«Статус» = [Клиент и операция найдены] и ФЛ, при наличии	В соответствии с международной системой и планом нумерации	Абонентский номер подвижной радиотелефонной связи получателя средств, подтвержденный в соответствии с п. 5.2.1 Положения № 683-П
7	Критерии легитимности операции без согласия, характеризующие получателя средств или плательщика	Критерии легитимности операции без согласия, характеризующие получателя средств или плательщика	УО	«Статус» = [Клиент и операция найдены] и получатель средств или плательщик соответствует хотя бы одному из критериев легитимности	Из классификатора «Критерии легитимности (признаки осуществления перевода денежных средств без согласия клиента) операции без согласия», приведенного в приложении 28	Выбираются все критерии легитимности операции без согласия, характеризующие получателя средств или плательщика
8	Информация о средстве платежа	Тип средства платежа	УО	«Статус» = [Клиент и операция найдены]	Выбор одного значения из списка: [Наличные] [Банковский счет] [Платежная карта] [Абонентский номер подвижной радиотелефонной связи] [Электронный кошелек]	-
9		Номер банковского счета	УО	«Статус» = [Клиент и операция найдены], [P2P-операция] и «Тип средства платежа» = [Банковский счет]	В соответствии с форматом, определенным Положением Банка России № 579-П	-
10		БИК оператора по переводу денежных средств			В соответствии с форматом, определенным Положением Банка России № 732-П	-
11		Номер платежной карты	УО	«Статус» = [Клиент и операция найдены], [P2P-операция] и «Тип средства платежа» = [Платежная карта]	В соответствии с форматом ISO/IEC 7812	-
12		Абонентский номер подвижной радиотелефонной связи	УО	«Статус» = [Клиент и операция найдены], [P2P-операция] и «Тип средства платежа» = [Абонентский номер подвижной радиотелефонной связи]	В соответствии с международной системой и планом нумерации	-
13		Идентификатор электронного кошелька	УО	«Статус» = [Клиент и операция найдены], [P2P-операция] и «Тип средства платежа» = [Электронный кошелек]	В соответствии с форматом идентификаторов электронных кошельков, определенных оператором электронных денежных средств	-

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
14		ИНН оператора электронных денежных средств, выпустившего электронный кошелек			В соответствии с форматом, утвержденным ФНС России	
15	Информация, используемая для идентификации устройств	Способ проведения операции	УО	При наличии информации о способе проведения операции	Выбор одного значения из списка: [ATM] [BRANCH] [DBO]. [MB] [DBO]. [WEB] [DBO]. [TC] [ECOM] [POS] [SST]	[ATM] – с использованием банкомата [BRANCH] – в отделении кредитной организации [DBO]. [MB] – с использованием мобильного банка [DBO]. [WEB] – с использованием банк-клиента (тонкий клиент) [DBO]. [TC] – с использованием банк-клиента (толстый клиент) [ECOM] – с использованием средств электронной коммерции [POS] – с использованием POS-терминала [SST] – с использованием терминала самообслуживания
16		Идентификатор устройства	УО	Поле «Способ проведения операции» = [ATM], [POS] или [SST]	Текстовое поле	Уникальный идентификатор устройства, с которого осуществлялась операция
17		Уникальный числовой идентификатор устройства в сети Интернет	УО	Поле «Способ проведения операции» = [DBO]. [MB], [DBO]. [WEB], [DBO]. [TC]	В соответствии с форматом RFC 791 или RFC 2460	IP-адрес устройства
18		Сетевой адрес компьютера и (или) коммуникационного устройства (маршрутизатора)	Н	-	В соответствии с форматом IEEE	MAC-адрес устройства
19		Международный идентификатор абонента (индивидуальный номер абонента – физического лица)	Н	-	В соответствии с форматом ITU-T E. 118	Номер сим-карты (ICCID)
20		Международный идентификатор пользовательского оборудования (оконечного оборудования) абонента – физического лица	Н	-	В соответствии с форматом ITU-T E. 212	IMSI устройства
21		Цифровой отпечаток устройства	Н	-	Цифровой отпечаток устройства, собранный в соответствии с рекомендациями Банка России	-
22	Приостановление зачисления денежных средств	Приостановление зачисления денежных средств	УО	REQ_OWC_ Identification: «Необходимость приостановления зачисления денежных средств» = [Да]	[Приостановлено] [Невозможно приостановить]	-

ПРИЛОЖЕНИЕ 5. ФОРМА ПРЕДСТАВЛЕНИЯ ДАННЫХ REQ_OWC_UUID – ФОРМА ЗАПРОСА БАНКА РОССИИ В ЦЕЛЯХ ПОЛУЧЕНИЯ ДАННЫХ ОБ ОПЕРАЦИИ БЕЗ СОГЛАСИЯ НА ОСНОВАНИИ СВЕДЕНИЙ О СОВЕРШЕННЫХ ПРОТИВОПРАВНЫХ ДЕЙСТВИЯХ ОТ ФЕДЕРАЛЬНОГО ОРГАНА ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ В СФЕРЕ ВНУТРЕННИХ ДЕЛ

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип запроса/ответа	Тип запроса/ответа	О	-	[REQ_OWC_UUID]	Предзаполненное поле
2	Информация, устанавливающая идентификаторы плательщика (идентифицирующая плательщика)	ИНН	О	Если ЮЛ, иначе при наличии	В соответствии с форматом ФНС России	Обязательно заполняется хотя бы одно из полей
3		Результат вычисления специального кода номера ДУЛ		Если ФЛ	Результат вычисления хеш-функции SHA-256	
4		Результат вычисления специального кода номера СНИЛС		Если ФЛ, при наличии	Результат вычисления хеш-функции SHA-256	
5		Абонентский номер подвижной радиотелефонной связи		Если ФЛ, при наличии	В соответствии с международной системой и планом нумерации	
6	Информация о способе проведения операции плательщиком	Номер платежной карты	УО	При операции плательщика с использованием платежной карты	В соответствии с форматом ISO/IEC 7812	-
7		Абонентский номер подвижной радиотелефонной связи	УО	При операции плательщика с использованием абонентского номера подвижной радиотелефонной связи или операции с использованием СБП (C2C, C2B, B2C)	В соответствии с международной системой и планом нумерации	-
8		Номер банковского счета	УО	При операции плательщика с использованием банковского счета или операции с использованием СБП (B2C, B2B)	В соответствии с форматом, определенным Положением Банка России № 579-П	-
9		БИК оператора по переводу денежных средств, обслуживающего плательщика			В соответствии с форматом, определенным Положением Банка России № 732-П	-
10		Идентификатор электронного кошелька	УО	При операции плательщика с использованием электронного кошелька	В соответствии с форматом идентификаторов электронных кошельков, определенных оператором электронных денежных средств	-
11		Наименование оператора электронных денежных средств, выпустившего электронный кошелек			Из перечня, формируемого на основании официального справочника операторов электронных денежных средств	-

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
12		Идентификатор банкомата или электронного терминала	УО	При операции плательщика в адрес торгово-сервисного предприятия или операции с использованием банкомата	В соответствии с форматом, утвержденным платежной системой	-
13		Адрес расположения банкомата или электронного терминала			В соответствии с структурой адреса ФИАС	-
14		Наименование оператора по переводу денежных средств, обслуживающего банкомат	УО	При операции с использованием банкомата	Из перечня, формируемого на основании официального справочника операторов по переводу денежных средств	-
15	Информация об способе получения денежных средств получателем	Номер платежной карты	УО	При операции с использованием платежной карты получателя	В соответствии с форматом ISO/IEC 7812	Заполняются при наличии информации о способе получения денежных средств получателем
16		Абонентский номер подвижной радиотелефонной связи	УО	При операции с использованием абонентского номера получателя	В соответствии с международной системой и планом нумерации	
17		Номер банковского счета	УО	При операции с использованием банковского счета получателя	В соответствии с форматом, определенным Положением Банка России № 579-П	
18		БИК оператора по переводу денежных средств, обслуживающего получателя			В соответствии с форматом, определенным Положением Банка России № 732-П	
19		Идентификатор электронного кошелька	УО	При операции с использованием электронного кошелька получателя	В соответствии с форматом идентификаторов электронных кошельков, определенных оператором электронных денежных средств	
20		Наименование оператора электронных денежных средств, выпустившего электронный кошелек			Из перечня, формируемого на основании официального справочника операторов электронных денежных средств	
21		ИНН торгово-сервисного предприятия	УО	При операции плательщика в адрес торгово-сервисного предприятия или операции с использованием СБП (C2B, B2B)	В соответствии с форматом, утвержденным ФНС России	
22		Идентификатор торгово-сервисного предприятия			В соответствии с форматом, утвержденным платежной системой	
23		Наименование оператора по переводу денежных средств, обслуживающего получателя	УО	При операции с использованием СБП	Из перечня, формируемого на основании официального справочника операторов по переводу денежных средств	

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
24	Информация, устанавливающая операцию	Дата и время операции	О	-	В соответствии с RFC 3339	По московскому времени [UTC +03:00]
25		Сумма операции	О	-	Сумма с точностью до двух знаков после запятой	-
26		Валюта операции	О	-	Из Общероссийского классификатора валют	-
27		Идентификатор операции СБП (номер операции)	УО	При операции плательщика с использованием СБП	В соответствии со стандартами ОПКЦ СБП	-
28		БИК оператора по переводу денежных средств – эквайрера	УО	При операции плательщика в адрес торгово-сервисного предприятия	В соответствии с форматом, определенным Положением Банка России № 732-П	-
29		Ссылочный номер операции (транзакции)	УО	При операции плательщика в адрес торгово-сервисного предприятия с использованием платежной карты	В соответствии с форматом, утвержденным платежной системой	Retrieval Reference Number (RRN)
30		Идентификатор фискального документа	УО	При операции плательщика в адрес торгово-сервисного предприятия	В соответствии с требованиями Федерального закона № 54-ФЗ	-
31	Дополнительные сведения о способе проведения операции	Дополнительные сведения о способе проведения операции	УО	При отсутствии вышеуказанной информации	Текстовое поле	Текстовое описание способа проведения операции
32	Информация об обращении клиента, связанного с осуществлением переводов денежных средств без согласия в федеральный орган исполнительной власти в сфере внутренних дел	Дата внесения в книгу учета сообщений о преступлениях	УО	В случае внесения в книгу учета сообщений о преступлениях	В соответствии с RFC 3339. По московскому времени [UTC +03:00]	Обязательно заполняется одна из пар полей
33		Порядковый номер в книге учета сообщений о преступлениях			В соответствии с форматом, установленным МВД России	
34		Дата заведения уголовного дела	УО	В случае заведения уголовного дела	В соответствии с RFC 3339. По московскому времени [UTC +03:00]	
35		Номер уголовного дела			В соответствии с форматом, установленным МВД России	

Форма представления данных RESP_OWC_UUID – Форма представления ответа на запрос Банка России в целях получения данных об операции без согласия на основании сведений о совершенных противоправных действиях от федерального органа исполнительной власти в сфере внутренних дел

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип запроса/ответа	Тип запроса/ответа	О	-	[RESP_OWC_UUID]	Предзаполненное поле

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
2	Статус	Статус	О	-	[ОБС уже направлена в Банк России] [Клиент не найден] [Операция не найдена] [Необходимо дополнительное время для рассмотрения]	-
3	Идентификатор уведомления об операции без согласия	Идентификатор уведомления об операции без согласия	УО	«Статус» = [ОБС направлена в Банк России]	В соответствии с форматом АСОИ ФинЦЕРТ	Идентификатор уведомления об операции без согласия, ранее направленного в ФинЦЕРТ участником информационного обмена

ПРИЛОЖЕНИЕ 6. ФОРМА ПРЕДСТАВЛЕНИЯ ДАННЫХ REQ_OWC_FORWARD – ФОРМА ЗАПРОСА БАНКА РОССИИ В ЦЕЛЯХ ПОЛУЧЕНИЯ ДАННЫХ О ДЕЙСТВИЯХ УЧАСТНИКА ИНФОРМАЦИОННОГО ОБМЕНА, ОБСЛУЖИВАЮЩЕГО ПОЛУЧАТЕЛЯ СРЕДСТВ, ПО ПЕРЕВОДУ ДЕНЕЖНЫХ СРЕДСТВ

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип запроса/ответа	Тип запроса/ответа	О	-	[REQ_OWC_Forward]	Предзаполненное поле
2	Информация об идентификаторах получателя средств (идентифицирующая получателя средств)	ИНН	УО	Если плательщик – юридическое лицо, иначе при наличии	В соответствии с форматом ФНС России	Обязательно заполняется хотя бы одно из полей
3		Результат вычисления специального кода номера ДУЛ	УО	Если плательщик – физическое лицо	Результат вычисления хеш-функции SHA-256	
4		Результат вычисления специального кода номера СНИЛС	УО	Если плательщик – физическое лицо, при наличии	Результат вычисления хеш-функции SHA-256	-
5		Абонентский номер подвижной радиотелефонной связи	УО	Если плательщик – физическое лицо, иначе при наличии	В соответствии с международной системой и планом нумерации	Абонентский номер подвижной радиотелефонной связи плательщика, подтвержденный в соответствии с п. 5.2.1 Положения № 683-П
6	Информация о средстве платежа получателя	Тип средства платежа получателя средств	О	-	Выбор одного значения из списка: [Наличные] [Банковский счет] [Платежная карта] [Абонентский номер подвижной радиотелефонной связи] [Электронный кошелек]	-
7		Номер банковского счета	УО	Поле «Тип средства платежа» = [Банковский счет]	В соответствии с форматом, определенным Положением Банка России № 579-П	-
8		БИК оператора по переводу денежных средств			В соответствии с форматом, определенным Положением Банка России № 732-П	-
9		Номер платежной карты	УО	Поле «Тип средства платежа» = [Платежная карта]	В соответствии с форматом ISO/IEC 7812	-
10		Абонентский номер подвижной радиотелефонной связи	УО	Поле «Тип средства платежа» = [Абонентский номер подвижной радиотелефонной связи]	В соответствии с международной системой и планом нумерации	-
11		Идентификатор электронного кошелька	УО	Поле «Тип средства платежа» = [Электронный кошелек]	В соответствии с форматом идентификаторов электронных кошельков, определенных оператором электронных денежных средств	-

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
12		ИНН оператора электронных денежных средств, выпустившего электронный кошелек			В соответствии с форматом, утвержденным ФНС России	-
13	Информация, устанавливающая операцию по переводу денежных средств	Дата и время операции	О	-	В соответствии с RFC 3339	По московскому времени [UTC +03:00]
14		Сумма операции	О	-	Сумма без учета комиссии банка с точностью до двух знаков после запятой	-
15		Валюта операции	О	-	Из Общероссийского классификатора валют	-
16		Идентификатор оператора по переводу денежных средств, обслуживающего плательщика, при использовании СПФС или SWIFT	УО	Поле «Технология осуществления перевода денежных средств» = [SPFS], [SWIFT]	В соответствии с форматом SWIFT	SWIFT-code плательщика
17		Идентификатор оператора по переводу денежных средств, обслуживающего получателя средств, при использовании СПФС или SWIFT			В соответствии с форматом SWIFT	SWIFT-code получателя средств
18		Идентификатор операции SWIFT (номер операции)			В соответствии с форматом SWIFT	-
19		Идентификатор торгово-сервисного предприятия	УО	При операции в адрес торгово-сервисного предприятия	В соответствии с форматом, утвержденным платежной системой	MerchantID
20		ИНН торгово-сервисного предприятия	УО	При операции в адрес торгово-сервисного предприятия, при наличии	В соответствии с форматом, утвержденным ФНС России	-
21		Ссылочный номер операции (транзакции)	УО	Поле «Технология осуществления перевода денежных средств» = [CARD]	В соответствии с форматом, утвержденным платежной системой	Retrieval Reference Number (RRN)
22		Код ответа операции (транзакции)			[Одобрена] [Отклонена]	Response Code
23		Код причины возврата			В соответствии с форматом, утвержденным платежной системой	Reason Code
24		BIN оператора по переводу денежных средств – эквайрера			В соответствии с форматом, утвержденным платежной системой	-
25		Код, отражающий основной вид деятельности торгово-сервисного предприятия	УО	Поле «Технология осуществления перевода денежных средств» = [CARD], и заполнение данного поля в авторизационных сообщениях предусмотрено стандартами ПС	В соответствии с форматом, утвержденным платежной системой	MCC

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
26		Значение токена при токенизированной операции	УО	Поле «Технология осуществления перевода денежных средств» = [CARD], и проводилась операция с токенизированной картой	В соответствии с форматом, утвержденным платежной системой	Token Number
27		Идентификатор СБП оператора по переводу денежных средств, обслуживающего получателя средств	УО	Поле «Технология осуществления перевода денежных средств» = [SBP]	В соответствии со стандартами ОПКЦ СБП	MemberID
28		Идентификатор операции СБП (номер операции)	УО	Поле «Технология осуществления перевода денежных средств» = [SBP]	В соответствии со стандартами ОПКЦ СБП	TR ID
29		Идентификатор платежной ссылки СБП	УО	Поле «Технология осуществления перевода денежных средств» = [SBP], «Тип операции» = [B2B], [C2B], [C2G], и операция выполнялась с использованием платежной ссылки	В соответствии со стандартами ОПКЦ СБП	QRC_ID
30	Сведения об анализе операции без согласия	Количество дней до и после указанной операции, за которые необходимо проанализировать операции получателя средств	Н	-	Целое число >0	-

Форма представления данных RESP_OWC_Forward – Форма представления ответа на запрос Банка России в целях получения данных о действиях участника информационного обмена, обслуживающего получателя средств, по переводу денежных средств

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип запроса/ответа	Тип запроса/ответа	О	-	[RESP_OWC_Forward]	Предзаполненное поле
2	Статус	Статус	О	-	[Клиент и операция найдены] [Клиент не найден] [Операция не найдена] [Необходимо дополнительное время для рассмотрения]	-
3	Элемент, на основании которого предоставлены сведения	Элемент REQ_OWC_Forward, на основании которого предоставлены сведения	УО	«Статус» = [Клиент и операция найдены]	Одно или совокупность указанных в запросе значений, разделенных;	-

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
4	Информация о способе проведения операции	Технология осуществления перевода денежных средств	УО	«Статус» = [Клиент и операция найдены]	Выбор одного значения из списка: [INT] [CARD] [WALLET] [PS BR] [SPFS] [SWIFT] [SBP] [MONEY] Перечень зависит от поля «Тип средства платежа плательщика»	[INT] – внутренний перевод [CARD] – карточные платежные системы [WALLET] – платежные системы без открытия счета [PS_BR] – межбанковские переводы с использованием ПС БР [SPFS] – межбанковские переводы с использованием СПФС [SWIFT] – межбанковские переводы с использованием SWIFT [SBP] – межбанковские переводы с использованием СБП [MONEY] – быстрые денежные переводы без открытия счета
5		Платежная система	УО	Поле «Статус» = [Клиент и операция найдены] и «Технология осуществления перевода денежных средств» = [CARD], [WALLET], [MONEY]	ИНН, в соответствии с форматом ФНС России, или [Иное]	В случае наличия ИНН у оператора платежной системы или оператора электронных денежных средств указывается ИНН, иначе значение [Иное]
6		Тип операции	УО	«Статус» = [Клиент и операция найдены]	«Выбор одного значения из списка: [FUND] [WITHDRAW] [TRANSFER] [CROSS] [PURCHASE] [CHARGEBACK] [B2B] [B2C] [C2B] [C2C] [C2G] Перечень зависит от полей «Тип средства платежа плательщика» и «Платежная система»	[FUND] – внесение наличных денежных средств [WITHDRAW] – снятие наличных денежных средств [TRANSFER] – перевод денежных средств между однотипными средствами платежа [CROSS] – перевод денежных средств с конвертацией между разнотипными средствами платежа [PURCHASE] – покупка [CHARGEBACK] – возврат [B2B] – B2B-операции в СБП [B2C] – B2C-операции в СБП [C2B] – C2B-операции в СБП [C2C] – C2C-операции в СБП [C2G] – C2G-операции в СБП

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
7	Информация о средстве платежа получателя	Тип средства платежа	УО	«Статус» = [Клиент и операция найдены]	Выбор одного значения из списка: [Наличные] [Банковский счет] [Платежная карта] [Абонентский номер подвижной радиотелефонной связи] [Электронный кошелек] Перечень зависит от полей «Платежная система» и «Тип операции»	-
8		Номер банковского счета	УО	Поле «Статус» = [Клиент и операция найдены] и «Тип средства платежа» = [Банковский счет]	В соответствии с форматом, определенным Положением Банка России № 579-П	-
9		БИК оператора по переводу денежных средств			В соответствии с форматом, определенным Положением Банка России № 732-П	-
10		Номер платежной карты	УО	Поле «Статус» = [Клиент и операция найдены] и «Тип средства платежа» = [Платежная карта]	В соответствии с форматом ISO/IEC 7812	-
11		Абонентский номер подвижной радиотелефонной связи	УО	Поле «Статус» = [Клиент и операция найдены] и «Тип средства платежа» = [Абонентский номер подвижной радиотелефонной связи]	В соответствии с международной системой и планом нумерации	-
12		Идентификатор электронного кошелька	УО	Поле «Статус» = [Клиент и операция найдены] и «Тип средства платежа» = [Электронный кошелек]	В соответствии с форматом идентификаторов электронных кошельков, определенных оператором электронных денежных средств	-
13		ИНН оператора электронных денежных средств, выпустившего электронный кошелек			В соответствии с форматом, утвержденным ФНС России	-
14	Информация об идентификаторах получателя средств (идентифицирующая получателя средств)	ИНН	УО	Поле «Технология осуществления перевода денежных средств» = [INT]	В соответствии с форматом ФНС России	Обязательно заполняется хотя бы одно из полей
15		Результат вычисления специального кода номера ДУЛ			Результат вычисления хеш-функции SHA-256	
16		Результат вычисления специального кода номера СНИЛС			Результат вычисления хеш-функции SHA-256	При наличии

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
17		Абонентский номер подвижной радиотелефонной связи			В соответствии с международной системой и планом нумерации	Абонентский номер подвижной радиотелефонной связи получателя средств, подтвержденный в соответствии с п. 5.2.1 Положения № 683-П
18	Информация, устанавливающая операцию по переводу денежных средств	Дата и время операции	УО	«Статус» = [Клиент и операция найдены]	В соответствии с RFC 3339	По московскому времени [UTC +03:00]
19		Сумма операции	УО	«Статус» = [Клиент и операция найдены]	Сумма без учета комиссии банка с точностью до двух знаков после запятой	-
20		Валюта операции	УО	«Статус» = [Клиент и операция найдены]	Из Общероссийского классификатора валют	-
21		Сумма операции в рублях по внутреннему курсу	УО	Поле «Валюта операции» ≠ [RUB]	Сумма с точностью до двух знаков после запятой	-
22		Назначение платежа	Н	-	Текстовое поле	-
23		БИК оператора по переводу денежных средств, обслуживающего получателя средств	УО	«Статус» = [Клиент и операция найдены]	В соответствии с форматом, определенным Положением Банка России № 732-П	-
24		Идентификатор оператора по переводу денежных средств, обслуживающего плательщика, при использовании СПФС или SWIFT	УО	Поле «Технология осуществления перевода денежных средств» = [SPFS], [SWIFT]	В соответствии с форматом SWIFT	SWIFT-code плательщика
25		Идентификатор оператора по переводу денежных средств, обслуживающего получателя средств, при использовании СПФС или SWIFT			В соответствии с форматом SWIFT	SWIFT-code получателя средств
26		Идентификатор операции SWIFT (номер операции)			В соответствии с форматом SWIFT	-
27		Идентификатор торгово-сервисного предприятия	УО	При операции в адрес торгово-сервисного предприятия	В соответствии с форматом, утвержденным платежной системой	MerchantID
28		ИНН торгово-сервисного предприятия	УО	При операции в адрес торгово-сервисного предприятия, при наличии	В соответствии с форматом, утвержденным ФНС России	-
29		Ссылочный номер операции (транзакции)	УО	Поле «Технология осуществления перевода денежных средств» = [CARD]	В соответствии с форматом, утвержденным платежной системой	Retrieval Reference Number (RRN)
30		Код ответа операции (транзакции)			[Одобрена] [Отклонена]	Response Code
31		Код причины возврата			В соответствии с форматом, утвержденным платежной системой	Reason Code

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
32		BIN оператора по переводу денежных средств – эквайрера			В соответствии с форматом, утвержденным платежной системой	-
33		Код, отражающий основной вид деятельности торгово-сервисного предприятия	УО	Поле «Технология осуществления перевода денежных средств» = [CARD], и заполнение данного поля в авторизационных сообщениях предусмотрено стандартами ПС	В соответствии с форматом, утвержденным платежной системой	MCC
34		Значение токена при токенизированной операции	УО	Поле «Технология осуществления перевода денежных средств» = [CARD], и проводилась операция с токенизированной картой	В соответствии с форматом, утвержденным платежной системой	Token Number
35		Идентификатор СБП оператора по переводу денежных средств, обслуживающего получателя средств	УО	Поле «Технология осуществления перевода денежных средств» = [SBP]	В соответствии со стандартами ОПКЦ СБП	MemberID
36		Идентификатор операции СБП (номер операции)	УО	Поле «Технология осуществления перевода денежных средств» = [SBP] и «Тип операции» = [C2C], [B2C]	В соответствии со стандартами ОПКЦ СБП	-
37		Идентификатор платежной ссылки СБП	УО	Поле «Технология осуществления перевода денежных средств» = [SBP] и «Тип операции» = [B2B], [C2B], и операция выполнялась с использованием платежной ссылки	В соответствии со стандартами ОПКЦ СБП	QRC_ID
38	Информация, используемая для идентификации устройств	Способ проведения операции	УО	«Статус» = [Клиент и операция найдены]	Выбор одного значения из списка: [ATM] [BRANCH] [DBO]. [MB] [DBO]. [WEB] [DBO]. [TC] [ECOM] [POS] [SST]	[ATM] – с использованием банкомата [BRANCH] – в отделении кредитной организации [DBO]. [MB] – с использованием мобильного банка [DBO]. [WEB] – с использованием банк-клиента (тонкий клиент) [DBO]. [TC] – с использованием банк-клиента (толстый клиент) [ECOM] – с использованием средств электронной коммерции [POS] – с использованием POS терминала [SST] – с использованием терминала самообслуживания

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
39		Идентификатор устройства	УО	Поле «Способ проведения операции» = [ATM], [POS] или [SST]	Текстовое поле	Уникальный идентификатор устройства, с которого осуществлялась операция
40		Адрес устройства или отделения кредитной организации	УО	Поле «Способ проведения операции» = [ATM], [BRANCH], [POS] или [SST]	Текстовое поле	Адрес устройства или отделения кредитной организации
41		Уникальный числовой идентификатор устройства в сети Интернет	УО	Поле «Способ проведения операции» = [DBO]. [MB], [DBO]. [WEB], [DBO]. [TC]	В соответствии с форматом RFC 791 или RFC 2460	IP-адрес устройства
42		Сетевой адрес компьютера и (или) коммуникационного устройства (маршрутизатора)	Н	-	В соответствии с форматом IEEE	MAC-адрес устройства
43		Международный идентификатор абонента (индивидуальный номер абонента – физического лица)	Н	-	В соответствии с форматом ITU-T E. 118	Номер сим-карты (ICCID)
44		Международный идентификатор пользовательского оборудования (оконечного оборудования) абонента – физического лица	Н	-	В соответствии с форматом ITU-T E. 212	IMSI устройства
45		Цифровой отпечаток устройства	Н	-	Цифровой отпечаток устройства, собранный в соответствии с рекомендациями Банка России	-
46		Фишинговый URL	Н	-	В соответствии с форматом RFC 3986	Заполняется в случае инициации транзакции с фишингового сайта
47	Критерии легитимности операции без согласия	Критерии легитимности операции без согласия	УО	Поле «Статус» = [Клиент и операция найдены], и операция соответствует хотя бы одному из критериев легитимности	Из классификатора «Критерии легитимности (признаки осуществления перевода денежных средств без согласия клиента) операции без согласия», приведенного в приложении 28	Выбираются все критерии легитимности операции без согласия

ПРИЛОЖЕНИЕ 7. ФОРМА ПРЕДСТАВЛЕНИЯ ДАННЫХ REQ_OWC_REVERSE – ФОРМА ЗАПРОСА БАНКА РОССИИ В ЦЕЛЯХ ПОЛУЧЕНИЯ ИНФОРМАЦИИ О ПЛАТЕЛЬЩИКАХ УКАЗАННОМУ В ЗАПРОСЕ БАНКА РОССИИ ПОЛУЧАТЕЛЮ СРЕДСТВ

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип запроса/ответа	Тип запроса/ответа	О	-	[REQ_OWC_Reverse]	Предзаполненное поле
2	Информация об идентификаторах получателя средств (идентифицирующая получателя средств)	ИНН	УО	Если плательщик – юридическое лицо, иначе при наличии	В соответствии с форматом ФНС России	Обязательно заполняется хотя бы одно из полей
3		Результат вычисления специального кода номера ДУЛ	УО	Если плательщик – физическое лицо	Результат вычисления хеш-функции SHA-256	
4		Результат вычисления специального кода номера СНИЛС	УО	Если плательщик – физическое лицо, при наличии	Результат вычисления хеш-функции SHA-256	-
5		Абонентский номер подвижной радиотелефонной связи	УО	Если плательщик – физическое лицо, иначе при наличии	В соответствии с международной системой и планом нумерации	Абонентский номер подвижной радиотелефонной связи плательщика, подтвержденный в соответствии с п. 5.2.1 Положения № 683-П
6	Информация о средстве платежа получателя	Тип средства платежа получателя средств	О	Поле «Тип операции» = [PURCHASE], [C2B], [B2B] заполняется при наличии	Выбор одного значения из списка: [Наличные] [Банковский счет] [Платежная карта] [Абонентский номер подвижной радиотелефонной связи] [Электронный кошелек]	-
7		Номер банковского счета	УО	Поле «Тип средства платежа» = [Банковский счет]	В соответствии с форматом, определенным Положением Банка России № 579-П	-
8		БИК оператора по переводу денежных средств			В соответствии с форматом, определенным Положением Банка России № 732-П	-
9		Номер платежной карты	УО	Поле «Тип средства платежа» = [Платежная карта]	В соответствии с форматом ISO/IEC 7812	-
10		Абонентский номер подвижной радиотелефонной связи	УО	Поле «Тип средства платежа» = [Абонентский номер подвижной радиотелефонной связи]	В соответствии с международной системой и планом нумерации	-
11		Идентификатор электронного кошелька	УО	Поле «Тип средства платежа» = [Электронный кошелек]	В соответствии с форматом идентификаторов электронных кошельков, определенных оператором электронных денежных средств	-

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
12		ИНН оператора электронных денежных средств, выпустившего электронный кошелек			В соответствии с форматом, утвержденным ФНС России	-
13	Информация, устанавливающая операцию по переводу денежных средств	Дата и время операции	О	-	В соответствии с RFC 3339	По московскому времени [UTC +03:00]
14		Сумма операции	О	-	Сумма без учета комиссии банка с точностью до двух знаков после запятой	-
15		Валюта операции	О	-	Из Общероссийского классификатора валют	-
16		Идентификатор оператора по переводу денежных средств, обслуживающего плательщика, при использовании СПФС или SWIFT	УО	Поле «Технология осуществления перевода денежных средств» = [SPFS], [SWIFT]	В соответствии с форматом SWIFT	SWIFT-code плательщика
17		Идентификатор оператора по переводу денежных средств, обслуживающего получателя средств, при использовании СПФС или SWIFT			В соответствии с форматом SWIFT	SWIFT-code получателя средств
18		Идентификатор операции SWIFT (номер операции)			В соответствии с форматом SWIFT	-
19		Идентификатор торгово-сервисного предприятия	УО	При операции в адрес торгово-сервисного предприятия	В соответствии с форматом, утвержденным платежной системой	MerchantID
20		ИНН торгово-сервисного предприятия	УО	При операции в адрес торгово-сервисного предприятия, при наличии	В соответствии с форматом, утвержденным ФНС России	-
21		Ссылочный номер операции (транзакции)	УО	Поле «Технология осуществления перевода денежных средств» = [CARD]	В соответствии с форматом, утвержденным платежной системой	Retrieval Reference Number (RRN)
22		Код ответа операции (транзакции)			[Одобрена] [Отклонена]	Response Code
23		Код причины возврата			В соответствии с форматом, утвержденным платежной системой	Reason Code
24		BIN оператора по переводу денежных средств – эквайрера			В соответствии с форматом, утвержденным платежной системой	-
25		Код, отражающий основной вид деятельности торгово-сервисного предприятия	УО	Поле «Технология осуществления перевода денежных средств» = [CARD], и заполнение данного поля в авторизационных сообщениях предусмотрено стандартами ПС	В соответствии с форматом, утвержденным платежной системой	MCC

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
26		Значение токена при токенизированной операции	УО	Поле «Технология осуществления перевода денежных средств» = [CARD], и проводилась операция с токенизированной картой	В соответствии с форматом, утвержденным платежной системой	Token Number
27		Идентификатор СБП оператора по переводу денежных средств, обслуживающего получателя средств	УО	Поле «Технология осуществления перевода денежных средств» = [SBP]	В соответствии со стандартами ОПКЦ СБП	MemberID
28		Идентификатор операции СБП (номер операции)	УО	Поле «Технология осуществления перевода денежных средств» = [SBP]	В соответствии со стандартами ОПКЦ СБП	TR ID
29		Идентификатор платежной ссылки СБП	УО	Поле «Технология осуществления перевода денежных средств» = [SBP], «Тип операции» = [B2B], [C2B], [C2G], и операция выполнялась с использованием платежной ссылки	В соответствии со стандартами ОПКЦ СБП	QRC_ID
30	Сведения об анализе операции без согласия	Количество дней до и после указанной операции, за которые необходимо проанализировать операции получателя средств	Н	-	Целое число >0	-

Форма представления данных RESP_OWC_Reverse – Форма представления ответа на запрос Банка России в целях получения информации о плательщиках указанному получателю средств

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип запроса/ответа	Тип запроса/ответа	О	-	[RESP_OWC_Reverse]	Предзаполненное поле
2	Статус	Статус	О	-	[Клиент и операция найдены] [Клиент не найден] [Операция не найдена] [Необходимо дополнительное время для рассмотрения]	-
3	Элемент, на основании которого предоставлены сведения	Элемент RESP_OWC_Reverse, на основании которого предоставлены сведения	УО	«Статус» = [Клиент и операция найдены]	Одно или совокупность указанных в запросе значений, разделенных «;»	-
4	Сведения о плательщике, осуществившем перевод денежных средств получателю средств, в зависимости от способа реализации перевода денежных средств	Тип средства платежа получателя средств	УО	«Статус» = [Клиент и операция найдены]	Выбор одного значения из списка: [Наличные] [Банковский счет] [Платежная карта] [Абонентский номер подвижной радиотелефонной связи] [Электронный кошелек]	-

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
5		Номер банковского счета	УО	Поле «Тип средства платежа» = [Банковский счет]	В соответствии с форматом, определенным Положением Банка России № 579-П	-
6		БИК оператора по переводу денежных средств			В соответствии с форматом, определенным Положением Банка России № 732-П	-
7		Номер платежной карты	УО	Поле «Тип средства платежа» = [Платежная карта]	В соответствии с форматом ISO/IEC 7812	-
8		Абонентский номер подвижной радиотелефонной связи	УО	Поле «Тип средства платежа» = [Абонентский номер подвижной радиотелефонной связи]	В соответствии с международной системой и планом нумерации	-
9		Идентификатор электронного кошелька	УО	Поле «Тип средства платежа» = [Электронный кошелек]	В соответствии с форматом идентификаторов электронных кошельков, определенных оператором электронных денежных средств	-
10		ИНН оператора электронных денежных средств, выпустившего электронный кошелек			В соответствии с форматом, утвержденным ФНС России	-
11	Критерии легитимности операции без согласия, характеризующие плательщика	Критерии легитимности операции без согласия, характеризующие плательщика	УО	Поле «Статус» = [Клиент и операция найдены], и плательщик соответствует хотя бы одному из критериев легитимности	Из классификатора «Критерии легитимности (признаки осуществления перевода денежных средств без согласия клиента) операции без согласия», приведенного в приложении 28	Выбираются все критерии легитимности операции без согласия, характеризующие плательщика
12	Информация о способе проведения операции	Технология осуществления перевода денежных средств	УО	«Статус» = [Клиент и операция найдены]	Выбор одного значения из списка: [INT] [CARD] [WALLET] [PS BR] [SPFS] [SWIFT] [SBP] [MONEY] Перечень зависит от поля «Тип средства платежа плательщика»	[INT] – внутренний перевод [CARD] – карточные платежные системы [WALLET] – платежные системы без открытия счета [PS_BR] – межбанковские переводы с использованием ПС БР [SPFS] – межбанковские переводы с использованием СПФС [SWIFT] – межбанковские переводы с использованием SWIFT [SBP] – межбанковские переводы с использованием СБП [MONEY] – быстрые денежные переводы без открытия счета

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
13		Платежная система	УО	Поле «Статус» = [Клиент и операция найдены] и «Технология осуществления перевода денежных средств» = [CARD], [WALLET], [MONEY]	ИНН, в соответствии с форматом ФНС России, или [Иное]	В случае наличия ИНН у оператора платежной системы или оператора электронных денежных средств указывается ИНН, иначе значение [Иное]
14		Тип операции	УО	«Статус» = [Клиент и операция найдены]	Выбор одного значения из списка: [FUND] [WITHDRAW] [TRANSFER] [CROSS] [PURCHASE] [CHARGEBACK] [B2B] [B2C] [C2B] [C2C] [C2G] Перечень зависит от полей «Тип средства платежа плательщика» и «Платежная система»	[FUND] – внесение наличных денежных средств [WITHDRAW] – снятие наличных денежных средств [TRANSFER] – перевод денежных средств между однотипными средствами платежа [CROSS] – перевод денежных средств с конвертацией между разнотипными средствами платежа [PURCHASE] – покупка [CHARGEBACK] – возврат [B2B] – B2B-операции в СБП [B2C] – B2C-операции в СБП [C2B] – C2B-операции в СБП [C2C] – C2C-операции в СБП [C2G] – C2G-операции в СБП
15	Информация, устанавливающая операцию по переводу денежных средств	Дата и время операции	О	«Статус» = [Клиент и операция найдены]	В соответствии с RFC 3339	По московскому времени [UTC +03:00]
16		Сумма операции	О	«Статус» = [Клиент и операция найдены]	Сумма без учета комиссии банка с точностью до двух знаков после запятой	-
17		Валюта операции	О	«Статус» = [Клиент и операция найдены]	Из Общероссийского классификатора валют	-
18		Идентификатор оператора по переводу денежных средств, обслуживающего плательщика, при использовании СПФС или SWIFT	УО	Поле «Технология осуществления перевода денежных средств» = [SPFS], [SWIFT]	В соответствии с форматом SWIFT	SWIFT-code плательщика
19		Идентификатор оператора по переводу денежных средств, обслуживающего получателя средств, при использовании СПФС или SWIFT			В соответствии с форматом SWIFT	SWIFT-code получателя средств
20		Идентификатор операции SWIFT (номер операции)			В соответствии с форматом SWIFT	-

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
21		Идентификатор торгово-сервисного предприятия	УО	При операции в адрес торгово-сервисного предприятия	В соответствии с форматом, утвержденным платежной системой	MerchantID
22		ИНН торгово-сервисного предприятия	УО	При операции в адрес торгово-сервисного предприятия, при наличии	В соответствии с форматом, утвержденным ФНС России	-
23		Ссылочный номер операции (транзакции)	УО	Поле «Технология осуществления перевода денежных средств» = [CARD]	В соответствии с форматом, утвержденным платежной системой	Retrieval Reference Number (RRN)
24		Код ответа операции (транзакции)			[Одобрена] [Отклонена]	Response Code
25		Код причины возврата			В соответствии с форматом, утвержденным платежной системой	Reason Code
26		BIN оператора по переводу денежных средств – эквайрера			В соответствии с форматом, утвержденным платежной системой	-
27		Код, отражающий основной вид деятельности торгово-сервисного предприятия	УО	Поле «Технология осуществления перевода денежных средств» = [CARD], и заполнение данного поля в авторизационных сообщениях предусмотрено стандартами ПС	В соответствии с форматом, утвержденным платежной системой	MCC
28		Значение токена при токенизированной операции	УО	Поле «Технология осуществления перевода денежных средств» = [CARD], и проводилась операция с токенизированной картой	В соответствии с форматом, утвержденным платежной системой	Token Number
29		Идентификатор СБП оператора по переводу денежных средств, обслуживающего получателя средств	УО	Поле «Технология осуществления перевода денежных средств» = [SBP]	В соответствии со стандартами ОПКЦ СБП	MemberID
30		Идентификатор операции СБП (номер операции)	УО	Поле «Технология осуществления перевода денежных средств» = [SBP] и «Тип операции» = [C2C], [B2C]	В соответствии со стандартами ОПКЦ СБП	-
31		Идентификатор платежной ссылки СБП	УО	Поле «Технология осуществления перевода денежных средств» = [SBP] и «Тип операции» = [B2B], [C2B], и операция выполнялась с использованием платежной ссылки	В соответствии со стандартами ОПКЦ СБП	QRC_ID

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
32	Критерии легитимности операции без согласия	Критерии легитимности операции без согласия	УО	Поле «Статус» = [Клиент и операция найдены], и операция соответствует хотя бы одному из критериев легитимности	Из классификатора «Критерии легитимности (признаки осуществления перевода денежных средств без согласия клиента) операции без согласия», приведенного в приложении 28	Выбираются все критерии легитимности операции без согласия

ПРИЛОЖЕНИЕ 8. ФОРМА ПРЕДСТАВЛЕНИЯ ДАННЫХ REQ_OWC_REVIEW – ФОРМА ЗАПРОСА УЧАСТНИКА ИНФОРМАЦИОННОГО ОБМЕНА В СЛУЧАЕ НЕОБОСНОВАННОГО НАПРАВЛЕНИЯ В БАНК РОССИИ ИНФОРМАЦИИ О ПЕРЕВОДАХ БЕЗ СОГЛАСИЯ КЛИЕНТА

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип уведомления	Тип уведомления	О	-	[REQ_OWC_Review]	Предзаполненное поле
2	Сведения, идентифицирующие клиента, находящегося в базе данных о случаях и попытках осуществления переводов денежных средств без согласия клиента	ИНН	УО	Если плательщик – юридическое лицо, иначе при наличии	В соответствии с форматом ФНС России	Обязательно заполняется хотя бы одно из полей
3		Результат вычисления специального кода номера ДУЛ	УО	Если плательщик – физическое лицо	Результат вычисления хеш-функции SHA-256	
4		Результат вычисления специального кода номера СНИЛС	УО	Если плательщик – физическое лицо, при наличии	Результат вычисления хеш-функции SHA-256	-
5		Абонентский номер подвижной радиотелефонной связи	УО	Если плательщик – физическое лицо, иначе при наличии	В соответствии с международной системой и планом нумерации	Абонентский номер подвижной радиотелефонной связи плательщика, подтвержденный в соответствии с п. 5.2.1 Положения № 683-П
6	Сведения о клиенте, находящемся в базе данных о случаях и попытках осуществления переводов денежных средств без согласия клиента, в зависимости от способа реализации перевода денежных средств	Номер банковского счета	УО	Поле «Тип средства платежа» = [Банковский счет]	В соответствии с форматом, определенным Положением Банка России № 579-П	Заполняются необходимые данные клиента, характеризующие средство платежа клиента, в зависимости от способа реализации перевода денежных средств. Обязательно заполняется одно из полей
7		БИК оператора по переводу денежных средств			В соответствии с форматом, определенным Положением Банка России № 732-П	
8		Номер платежной карты	УО	Поле «Тип средства платежа» = [Платежная карта]	В соответствии с форматом ISO/IEC 7812	
9		Абонентский номер подвижной радиотелефонной связи	УО	Поле «Тип средства платежа» = [Абонентский номер подвижной радиотелефонной связи]	В соответствии с международной системой и планом нумерации	
10		Идентификатор электронного кошелька	УО	Поле «Тип средства платежа» = [Электронный кошелек]	В соответствии с форматом идентификаторов электронных кошельков, определенных оператором электронных денежных средств	

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
11		ИНН оператора электронных денежных средств, выпустившего электронный кошелек			В соответствии с форматом, утвержденным ФНС России	
12		Идентификатор торгово-сервисного предприятия	УО	При операции в адрес торгово-сервисного предприятия	В соответствии с форматом, утвержденным платежной системой	
13		ИНН торгово-сервисного предприятия	УО	При операции в адрес торгово-сервисного предприятия, при наличии	В соответствии с форматом, утвержденным ФНС России	
14	Мотивированное обоснование	Мотивированное обоснование	О	-	Текстовое поле	-

Форма представления данных RESP_OWC_Review – Форма представления ответа на запрос участника информационного обмена в случае необоснованного направления в Банк России информации о переводах без согласия клиента

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип уведомления	Тип уведомления	О	-	[RESP_OWC_Review]	Предзаполненное поле
2	Статус рассмотрения запроса	Статус рассмотрения запроса	О	-	[Принято] [Отклонено]	-
3	Сведения, идентифицирующие клиента, удаленные из базы данных о случаях и попытках осуществления переводов денежных средств без согласия клиента	ИНН	УО	Если плательщик – юридическое лицо, иначе при наличии	В соответствии с форматом ФНС России	Обязательно заполняется одно из полей
4		Результат вычисления специального кода номера ДУЛ	УО	Если плательщик – физическое лицо	Результат вычисления хеш-функции SHA-256	
5		Результат вычисления специального кода номера СНИЛС	УО	Если плательщик – физическое лицо, при наличии	Результат вычисления хеш-функции SHA-256	
6		Абонентский номер подвижной радиотелефонной связи	УО	Если плательщик – физическое лицо, иначе при наличии	В соответствии с международной системой и планом нумерации	
7	Сведения о клиенте, исключенном из базы данных о случаях и попытках осуществления переводов денежных средств без согласия клиента, в зависимости от способа реализации перевода денежных средств	Номер банковского счета	УО	Поле «Тип средства платежа» = [Банковский счет]	В соответствии с форматом, определенным Положением Банка России № 579-П	Заполняются необходимые данные клиента, характеризующие средство платежа клиента, в зависимости от способа реализации перевода денежных средств
8		БИК оператора по переводу денежных средств			В соответствии с форматом, определенным Положением Банка России № 732-П	
9		Номер платежной карты	УО	Поле «Тип средства платежа» = [Платежная карта]	В соответствии с форматом ISO/IEC 7812	

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
10		Абонентский номер подвижной радиотелефонной связи	УО	Поле «Тип средства платежа» = [Абонентский номер подвижной радиотелефонной связи]	В соответствии с международной системой и планом нумерации	
11		Идентификатор электронного кошелька	УО	Поле «Тип средства платежа» = [Электронный кошелек]	В соответствии с форматом идентификаторов электронных кошельков, определенных оператором электронных денежных средств	
12		ИНН оператора электронных денежных средств, выпустившего электронный кошелек			В соответствии с форматом, утвержденным ФНС России	
13		Идентификатор торгово-сервисного предприятия	УО	При операции в адрес торгово-сервисного предприятия	В соответствии с форматом, утвержденным платежной системой	
14		ИНН торгово-сервисного предприятия	УО	При операции в адрес торгово-сервисного предприятия, при наличии	В соответствии с форматом, утвержденным ФНС России	
15	Обоснование	Обоснование	УО	«Статус рассмотрения запроса» = [Отклонено] или при необходимости	Текстовое поле	-

ПРИЛОЖЕНИЕ 9. ФОРМА ПРЕДСТАВЛЕНИЯ ДАННЫХ REQ_OWC_CORRECTION – ФОРМА ЗАПРОСА БАНКА РОССИИ О ПОВТОРНОМ НАПРАВЛЕНИИ ИНФОРМАЦИИ О ПЕРЕВОДАХ БЕЗ СОГЛАСИЯ КЛИЕНТА

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип запроса/ответа	Тип запроса/ответа	О	-	[REQ_OWC_Correction]	Предзаполненное поле
2	Идентификатор уведомления или ответа	Идентификатор уведомления или ответа участника информационного обмена	О	-	В соответствии с форматом АСОИ ФинЦЕРТ	Идентификатор уведомления или ответа на запрос, ранее направленного в ФинЦЕРТ участником информационного обмена и содержащего сведения, требующие уточнения или корректировки
3	Статус	Статус	О	-	[Клиент не найден] [Операция не найдена]	-
4	Сведения, требующие уточнения	ИНН	УО	Заполняются поля из уведомления или ответа участника информационного обмена, требующие уточнения. Заполняется как минимум одно из полей	В соответствии с форматом ФНС России	Обязательно заполняется хотя бы одно из полей
5		Результат вычисления специального кода номера ДУЛ			Результат вычисления хеш-функции SHA-256	
6		Результат вычисления специального кода номера СНИЛС			Результат вычисления хеш-функции SHA-256	-
7		Абонентский номер подвижной радиотелефонной связи			В соответствии с международной системой и планом нумерации	Абонентский номер подвижной радиотелефонной связи плательщика, подтвержденный в соответствии с п. 5.2.1 Положения № 683-П
8		Номер банковского счета			В соответствии с форматом, определенным Положением Банка России № 579-П	-
9		БИК оператора по переводу денежных средств			В соответствии с форматом, определенным Положением Банка России № 732-П	-
10		Номер платежной карты			В соответствии с форматом ISO/IEC 7812	-
11		Абонентский номер подвижной радиотелефонной связи			В соответствии с международной системой и планом нумерации	-

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
12		Идентификатор электронного кошелька			В соответствии с форматом идентификаторов электронных кошельков, определенных оператором электронных денежных средств	-
13		ИНН оператора электронных денежных средств, выпустившего электронный кошелек			В соответствии с форматом, утвержденным ФНС России	-
14		Дата и время операции			В соответствии с RFC 3339	По московскому времени [UTC +03:00]
15		Сумма операции			Сумма без учета комиссии банка с точностью до двух знаков после запятой	-
16		Валюта операции			Из Общероссийского классификатора валют	-
17		Сумма операции в рублях по внутреннему курсу			Сумма с точностью до двух знаков после запятой	-
18		Назначение платежа			Текстовое поле	-
19		БИК оператора по переводу денежных средств, обслуживающего получателя средств			В соответствии с форматом, определенным Положением Банка России № 732-П	-
20		Идентификатор оператора по переводу денежных средств, обслуживающего плательщика, при использовании СПФС или SWIFT			В соответствии с форматом SWIFT	SWIFT-code плательщика
21		Идентификатор оператора по переводу денежных средств, обслуживающего получателя средств, при использовании СПФС или SWIFT			В соответствии с форматом SWIFT	SWIFT-code получателя средств
22		Идентификатор операции SWIFT (номер операции)			В соответствии с форматом SWIFT	-
23		Идентификатор торгово-сервисного предприятия			В соответствии с форматом, утвержденным платежной системой	MerchantID
24		ИНН торгово-сервисного предприятия			В соответствии с форматом, утвержденным ФНС России	-
25		Ссылочный номер операции (транзакции)			В соответствии с форматом, утвержденным платежной системой	Retrieval Reference Number (RRN)
26		Код ответа операции (транзакции)			[Одобрена] [Отклонена]	Response Code
27		Код причины возврата			В соответствии с форматом, утвержденным платежной системой	Reason Code

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
28		BIN оператора по переводу денежных средств – эквайрера			В соответствии с форматом, утвержденным платежной системой	-
29		Код, отражающий основной вид деятельности торгово-сервисного предприятия			В соответствии с форматом, утвержденным платежной системой	MCC
30		Значение токена при токенизированной операции			В соответствии с форматом, утвержденным платежной системой	Token Number
31		Идентификатор СБП оператора по переводу денежных средств, обслуживающего получателя средств			В соответствии со стандартами ОПКЦ СБП	MemberID
32		Идентификатор операции СБП (номер операции)			В соответствии со стандартами ОПКЦ СБП	-
33		Идентификатор платежной ссылки СБП			В соответствии со стандартами ОПКЦ СБП	QRC_ID

Форма представления данных RESP_OWC_Correction – Форма представления ответа на запрос Банка России о повторном направлении информации о переводах без согласия клиента

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип запроса/ответа	Тип запроса/ответа	О	-	[RESP_OWC_ Correction]	Предзаполненное поле
2	Уточненные или скорректированные сведения по операции	ИНН	УО	Обязательно заполняется хотя бы одно из полей. Заполняются поля, входящие в состав запроса на уточнение или корректировку, ранее направленного участнику информационного обмена, которые были уточнены или скорректированы	В соответствии с форматом ФНС России	Обязательно заполняется хотя бы одно из полей
3		Результат вычисления специального кода номера ДУЛ			Результат вычисления хеш-функции SHA-256	
4		Результат вычисления специального кода номера СНИЛС			Результат вычисления хеш-функции SHA-256	-
5		Абонентский номер подвижной радиотелефонной связи			В соответствии с международной системой и планом нумерации	Абонентский номер подвижной радиотелефонной связи плательщика, подтвержденный в соответствии с п. 5.2.1 Положения № 683-П
6		Номер банковского счета			В соответствии с форматом, определенным Положением Банка России № 579-П	-

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
7		БИК оператора по переводу денежных средств			В соответствии с форматом, определенным Положением Банка России № 732-П	-
8		Номер платежной карты			В соответствии с форматом ISO/IEC 7812	-
9		Абонентский номер подвижной радиотелефонной связи			В соответствии с международной системой и планом нумерации	-
10		Идентификатор электронного кошелька			В соответствии с форматом идентификаторов электронных кошельков, определенных оператором электронных денежных средств	-
11		ИНН оператора электронных денежных средств, выпустившего электронный кошелек			В соответствии с форматом, утвержденным ФНС России	-
12		Дата и время операции			В соответствии с RFC 3339	По московскому времени [UTC +03:00]
13		Сумма операции			Сумма без учета комиссии банка с точностью до двух знаков после запятой	-
14		Валюта операции			Из Общероссийского классификатора валют	-
15		Сумма операции в рублях по внутреннему курсу			Сумма с точностью до двух знаков после запятой	-
16		Назначение платежа			Текстовое поле	-
17		БИК оператора по переводу денежных средств, обслуживающего получателя средств			В соответствии с форматом, определенным Положением Банка России № 732-П	-
18		Идентификатор оператора по переводу денежных средств, обслуживающего плательщика, при использовании СПФС или SWIFT			В соответствии с форматом SWIFT	SWIFT-code плательщика
19		Идентификатор оператора по переводу денежных средств, обслуживающего получателя средств, при использовании СПФС или SWIFT			В соответствии с форматом SWIFT	SWIFT-code получателя средств
20		Идентификатор операции SWIFT (номер операции)			В соответствии с форматом SWIFT	-
21		Идентификатор торгово-сервисного предприятия			В соответствии с форматом, утвержденным платежной системой	MerchantID

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
22		ИНН торгово-сервисного предприятия			В соответствии с форматом, утвержденным ФНС России	-
23		Ссылочный номер операции (транзакции)			В соответствии с форматом, утвержденным платежной системой	Retrieval Reference Number (RRN)
24		Код ответа операции (транзакции)			[Одобрена] [Отклонена]	Response Code
25		Код причины возврата			В соответствии с форматом, утвержденным платежной системой	Reason Code
26		BIN оператора по переводу денежных средств – эквайрера			В соответствии с форматом, утвержденным платежной системой	-
27		Код, отражающий основной вид деятельности торгово-сервисного предприятия			В соответствии с форматом, утвержденным платежной системой	MCC
28		Значение токена при токенизированной операции			В соответствии с форматом, утвержденным платежной системой	Token Number
29		Идентификатор СБП оператора по переводу денежных средств, обслуживающего получателя средств			В соответствии со стандартами ОПКЦ СБП	MemberID
30		Идентификатор операции СБП (номер операции)			В соответствии со стандартами ОПКЦ СБП	-
31		Идентификатор платежной ссылки СБП			В соответствии со стандартами ОПКЦ СБП	QRC_ID

ПРИЛОЖЕНИЕ 10. ФОРМА ПРЕДСТАВЛЕНИЯ ДАННЫХ NTF_OWC_DATAUPDATE – ФОРМА ПРЕДСТАВЛЕНИЯ УЧАСТНИКАМИ ИНФОРМАЦИОННОГО ОБМЕНА ДОПОЛНИТЕЛЬНЫХ И (ИЛИ) УТОЧНЯЮЩИХ СВЕДЕНИЙ ПО РАНЕЕ НАПРАВЛЕННОЙ ИНФОРМАЦИИ О ПЕРЕВОДАХ БЕЗ СОГЛАСИЯ КЛИЕНТА (О ПРЕКРАЩЕНИИ ДЕЙСТВИЯ БАНКОВСКОГО СЧЕТА, ПЛАТЕЖНОЙ КАРТЫ, ДОГОВОРА АБОНЕНТСКОГО ОБСЛУЖИВАНИЯ ПОДВИЖНОЙ РАДИОТЕЛЕФОННОЙ СВЯЗИ ИЛИ ЭЛЕКТРОННОГО СРЕДСТВА ПЛАТЕЖА, А ТАКЖЕ ЗАМЕНЕ НОМЕРА ДОКУМЕНТА, УДОСТОВЕРЯЮЩЕГО ЛИЧНОСТЬ, ИЛИ АБОНЕНТСКОГО НОМЕРА ПОДВИЖНОЙ РАДИОТЕЛЕФОННОЙ СВЯЗИ КЛИЕНТА, НАХОДЯЩЕГОСЯ В БАЗЕ ДАННЫХ О СЛУЧАЯХ И ПОПЫТКАХ ОСУЩЕСТВЛЕНИЯ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ БЕЗ СОГЛАСИЯ КЛИЕНТА)

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип уведомления	Тип уведомления	О	-	[NTF_OWC_DataUpdate]	Предзаполненное поле
2	Тип операции	Тип модификации сведений о клиенте	О	-	[EXPIRE] [BLOCK] [REPLACE]	[EXPIRE] – в случае прекращения действия платежной карты или электронного средства платежа в связи с истечением срока действия [BLOCK] – в случае прекращения действия банковского счета, платежной карты, договора абонентского обслуживания подвижной радиотелефонной связи или электронного средства платежа в связи с блокировкой [REPLACE] – в случае замены номера документа, удостоверяющего личность, или абонентского номера подвижной радиотелефонной связи клиента
3	Дата и время	Дата и время прекращения действия/замены	О	-	В соответствии с RFC 3339	По московскому времени [UTC +03:00]
4	Идентификационные данные клиента	Результат вычисления специального кода номера ДУЛ	УО	Если ФЛ	Результат вычисления хеш-функции SHA-256	Обязательно заполняется одно из полей
5		ИНН		Если ЮЛ	В соответствии с форматом ФНС России	
6	Сведения о клиенте, потерявшие актуальность в связи с прекращением действия или заменой	Номер банковского счета	УО	В случае прекращения действия банковского счета	В соответствии с форматом, определенным Положением Банка России № 579-П	-
7		Номер платежной карты	УО	В случае прекращения действия платежной карты	В соответствии с форматом ISO/IEC 7812	-
8		Абонентский номер подвижной радиотелефонной связи	УО	В случае прекращения действия или замены абонентского номера подвижной радиотелефонной связи	В соответствии с российской системой и планом нумерации	-

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
9		Идентификатор электронного кошелька	УО	В случае прекращения действия электронного кошелька	В соответствии с форматом идентификаторов электронных кошельков, определенных оператором электронных денежных средств	-
10		Наименование оператора электронных денежных средств, выпустившего электронный кошелек	УО	Поле «Идентификатор электронного кошелька» заполнено. Обязательно заполняется одно из полей	Из перечня операторов электронных денежных средств, размещенного на сайте Банка России	-
11		ИНН оператора электронных денежных средств, выпустившего электронный кошелек			В соответствии с форматом, утвержденным ФНС России	-
12	Актуальные сведения	Результат вычисления специального кода номера ДУЛ	УО	«Тип модификации сведений о клиенте» = [REPLACE] и замена номера документа, удостоверяющего личность	Результат вычисления хеш-функции SHA-256	-
13		Абонентский номер подвижной радиотелефонной связи		«Тип модификации сведений о клиенте» = [REPLACE], и замена абонентского номера подвижной радиотелефонной связи	В соответствии с российской системой и планом нумерации	-

ПРИЛОЖЕНИЕ 11. ПЕРЕЧЕНЬ ТИПОВ ИНЦИДЕНТОВ ЗАЩИТЫ ИНФОРМАЦИИ, СОГЛАСОВАННЫЙ С ФЕДЕРАЛЬНЫМ ОРГАНОМ ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ, УПОЛНОМОЧЕННЫМ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ, И ИНЦИДЕНТОВ ОПЕРАЦИОННОЙ НАДЕЖНОСТИ В РАЗРЕЗЕ ВИДОВ ДЕЯТЕЛЬНОСТИ КРЕДИТНЫХ ОРГАНИЗАЦИЙ, НЕКРЕДИТНЫХ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ И СУБЪЕКТОВ НАЦИОНАЛЬНОЙ ПЛАТЕЖНОЙ СИСТЕМЫ И СОСТАВЛЯЮЩИХ ИХ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
[BANK]	Деятельность кредитной организации и небанковской кредитной организации	[UNI] [BASE] [RNKO] [PNKO] [NDKO]	Кредитная организация с универсальной лицензией Кредитная организация с базовой лицензией Расчетная небанковская кредитная организация Платежная небанковская кредитная организация Небанковская депозитно-кредитная организация	[accept OrWithdrawal FundsPP]	Технологический процесс, обеспечивающий привлечение денежных средств физических лиц во вклады	[DT_BAC]	[DT_BAC_BANK_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением)	Выявление факта превышения допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением)	-

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
							[DT_BAC_BANK_2]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением), а также допустимого времени простоя и (или) деградации технологического процесса, установленного кредитной организацией (сигнальным значением), не превышающего 2 часов для банков, размер активов которых составляет более 500 миллиардов рублей и более, 4 часов для банков с универсальной лицензией, размер активов которого составляет менее 500 миллиардов рублей, на период более 6 часов для банков с базовой лицензией	Выявление факта превышения допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением), а также допустимого времени простоя и (или) деградации технологического процесса, установленного кредитной организацией (сигнальным значением), не превышающего 2 часов для банков, размер активов которых составляет более 500 миллиардов рублей и более, 4 часов для банков с универсальной лицензией, размер активов которого составляет менее 500 миллиардов рублей, 6 часов для банков с базовой лицензией	-
				[acceptOrWithdrawalFundsLP]	Технологический процесс, обеспечивающий привлечение денежных средств юридических лиц во вклады	[DT_BAC]	[DT_BAC_BANK_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением)	Выявление факта превышения допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением)	-

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
							[DT_BAC_BANK_3]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением), а также допустимого времени простоя и (или) деградации технологического процесса, установленного кредитной организацией (сигнальным значением), не превышающего 2 часов для банков, размер активов которых составляет более 500 миллиардов рублей и более, 4 часов для банков с универсальной лицензией, размер активов которого составляет менее 500 миллиардов рублей, 6 часов для банков с базовой лицензией, 6 часов для небанковских кредитных организаций	Выявление факта превышения допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением), а также допустимого времени простоя и (или) деградации технологического процесса, установленного кредитной организацией (сигнальным значением), не превышающего 2 часов для банков, размер активов которых составляет более 500 миллиардов рублей и более, 4 часов для банков с универсальной лицензией, размер активов которого составляет менее 500 миллиардов рублей, 6 часов для банков с базовой лицензией, 6 часов для небанковских кредитных организаций	-
				[placementOfFunds]	Технологический процесс, обеспечивающий размещение привлеченных во вклады денежных средств физических и (или) юридических лиц от своего имени и за свой счет	[BAC]	[BAC_BANK_4]	Инцидент, связанный с размещением привлеченных во вклады денежных средств физических и (или) юридических лиц от своего имени и за свой счет в результате НСД к объектам информационной инфраструктуры кредитной организации	Выявление событий, связанных с размещением привлеченных во вклады денежных средств физических и (или) юридических лиц от своего имени и за свой счет в результате НСД к объектам информационной инфраструктуры кредитной организации и, которые фиксируются кредитной организацией в базе данных о событиях операционного риска и потерях, понесенных вследствие его реализации, в соответствии с п. 1.2 Положения 716-П	Нет требования к бизнес-данным инцидента защиты информации

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
						[DT_BAC]	[DT_BAC_BANK_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением)	Выявление факта превышения допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением)	-
							[DT_BAC_BANK_3]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением), а также допустимого времени простоя и (или) деградации технологического процесса, установленного кредитной организацией (сигнальным значением), не превышающего 2 часов для банков, размер активов которых составляет более 500 миллиардов рублей и более, 4 часов для банков с универсальной лицензией, размер активов которого составляет менее 500 миллиардов рублей, 6 часов для банков с базовой лицензией, 6 часов для небанковских кредитных организаций	Выявление факта превышения допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением), а также допустимого времени простоя и (или) деградации технологического процесса, установленного кредитной организацией (сигнальным значением), не превышающего 2 часов для банков, размер активов которых составляет более 500 миллиардов рублей и более, 4 часов для банков с универсальной лицензией, размер активов которого составляет менее 500 миллиардов рублей, 6 часов для банков с базовой лицензией, 6 часов для небанковских кредитных организаций	-

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
				[maintainAccountPP]	Технологический процесс, обеспечивающий открытие и ведение банковских счетов физических лиц	[BAC]	[BAC_BANK_3]	Инцидент, связанный с изменением остатка на банковском счете в результате НСД к информационной инфраструктуре кредитной организации	Выявление событий, связанных с изменением остатка на банковском счете в результате НСД к информационной инфраструктуре кредитной организации, которые фиксируются кредитной организацией в базе данных о событиях операционного риска и потерях, понесенных вследствие его реализации, в соответствии с п. 1.2 Положения 716-П	Нет требования к бизнес-данным инцидента защиты информации
						[DT_BAC]	[DT_BAC_BANK_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением)	Выявление факта превышения допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением)	-
							[DT_BAC_BANK_4]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением), а также допустимого времени простоя и (или) деградации технологического процесса, установленного кредитной организацией (сигнальным значением), не превышающего 2 часов (за исключение небанковских кредитных организаций)	Выявление факта превышения допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением), а также допустимого времени простоя и (или) деградации технологического процесса, установленного кредитной организацией (сигнальным значением), не превышающего 2 часов (за исключение небанковских кредитных организаций)	-

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
				[maintainAccountLP]	Технологический процесс, обеспечивающий открытие и ведение банковских счетов юридических лиц	[BAC]	[BAC_BANK_3]	Инцидент, связанный с изменением остатка на банковском счете в результате НСД к информационной инфраструктуре кредитной организации	Выявление событий, связанных с изменением остатка на банковском счете в результате НСД к инфраструктуре кредитной организации, которые фиксируются кредитной организацией в базе данных о событиях операционного риска и потерях, понесенных вследствие его реализации, в соответствии с п. 1.2 Положения 716-П	Нет требования к бизнес-данным инцидента защиты информации
						[DT_BAC]	[DT_BAC_BANK_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением)	Выявление факта превышения допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением)	-
							[DT_BAC_BANK_5]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением), а также допустимого времени простоя и (или) деградации технологического процесса, установленного кредитной организацией (сигнальным значением), не превышающего 2 часов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением), а также допустимого времени простоя и (или) деградации технологического процесса, установленного кредитной организацией (сигнальным значением), не превышающего 2 часов	-

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
				[transferOfFundsByOrderPP]	Технологический процесс, обеспечивающий осуществление переводов денежных средств по поручению физических лиц по их банковским счетам	[MTR]	[MTR_OPDS_1]	Инцидент, связанный с осуществлением перевода денежных средств на основании несанкционированно модифицированного распоряжения клиента ОПДС	Выявление инцидентов, связанных с осуществлением перевода денежных средств на основании несанкционированно модифицированного распоряжения клиента ОПДС, которые фиксируются кредитной организацией в базе данных о событиях операционного риска и потерях, понесенных вследствие его реализации, в соответствии с п. 1.2 Положения 716-П	Нет требования к бизнес-данным инцидента защиты информации
							[MTR_OPDS_2]	Инцидент, связанный с осуществлением перевода денежных средств с искаженными реквизитами в результате НСД к объектам информационной инфраструктуры ОПДС	Выявление инцидентов, связанных с осуществлением переводов денежных средств с искаженными реквизитами в результате НСД к объектам информационной инфраструктуры ОПДС, которые фиксируются кредитной организацией в базе данных о событиях операционного риска и потерях, понесенных вследствие его реализации, в соответствии с п. 1.2 Положения 716-П	Нет требования к бизнес-данным инцидента защиты информации
						[DT_MTR]	[DT_MTR_OPDS_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением)	Выявление факта превышения допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением)	-

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
							[DT_MTR_OPDS_2]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением), а также допустимого времени простоя и (или) деградации технологического процесса, установленного кредитной организацией (сигнальным значением), не превышающего 2 часов для банков, размер активов которых составляет более 500 миллиардов рублей и более или признанных значимыми на рынке платежных услуг, 4 часов для банков с универсальной лицензией, размер активов которого составляет менее 500 миллиардов рублей, 6 часов для банков с базовой лицензией	Выявление факта превышения допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением), а также допустимого времени простоя и (или) деградации технологического процесса, установленного кредитной организацией (сигнальным значением), не превышающего 2 часов для банков, размер активов которых составляет более 500 миллиардов рублей и более или признанных значимыми на рынке платежных услуг, 4 часов для банков с универсальной лицензией, размер активов которого составляет менее 500 миллиардов рублей, 6 часов для банков с базовой лицензией	-
				[transferOfFundsByOrderLP]	Технологический процесс, обеспечивающий осуществление переводов денежных средств по поручению юридических лиц, в том числе банков-корреспондентов, по их банковским счетам, за исключением переводов по распоряжениям участников платежной системы	[MTR]	[MTR_OPDS_1]	Инцидент, связанный с осуществлением перевода денежных средств на основании несанкционированно модифицированного распоряжения клиента ОПДС	Выявление инцидентов, связанных с осуществлением перевода денежных средств на основании несанкционированно модифицированного распоряжения клиента ОПДС, которые фиксируются кредитной организацией в базе данных о событиях операционного риска и потерях, понесенных вследствие его реализации, в соответствии с п. 1.2 Положения 716-П	Нет требования к бизнес-данным инцидента защиты информации

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
							[MTR_OPDS_2]	Инцидент, связанный с осуществлением перевода денежных средств с искаженными реквизитами в результате НСД к объектам информационной инфраструктуры ОПДС	Выявление инцидентов, связанных с осуществлением переводов денежных средств с искаженными реквизитами в результате НСД к объектам информационной инфраструктуры ОПДС, которые фиксируются кредитной организацией в базе данных о событиях операционного риска и потерях, понесенных вследствие его реализации, в соответствии с п. 1.2 Положения 716-П	Нет требования к бизнес-данным инцидента защиты информации
						[DT_MTR]	[DT_MTR_OPDS_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением)	Выявление факта превышения допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением)	-

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
							[DT_MTR_OPDS_3]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением), а также допустимого времени простоя и (или) деградации технологического процесса, установленного кредитной организацией (сигнальным значением), не превышающего 2 часов для банков, размер активов которых составляет более 500 миллиардов рублей и более или признанных значимыми на рынке платежных услуг, 4 часов для банков с универсальной лицензией, размер активов которого составляет менее 500 миллиардов рублей, 6 часов для банков с базовой лицензией и небанковских кредитных организаций	Выявление факта превышения допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением), а также допустимого времени простоя и (или) деградации технологического процесса, установленного кредитной организацией (сигнальным значением), не превышающего 2 часов для банков, размер активов которых составляет более 500 миллиардов рублей и более или признанных значимыми на рынке платежных услуг, 4 часов для банков с универсальной лицензией, размер активов которого составляет менее 500 миллиардов рублей, 6 часов для банков с базовой лицензией и небанковских кредитных организаций	-
				[transferOfFunds-WithoutAccount]	Технологический процесс, обеспечивающий осуществление переводов денежных средств без открытия банковских счетов, в том числе электронных денежных средств (за исключением почтовых переводов)	[MTR]	[MTR_OPDS_3]	Инцидент, связанный с осуществлением перевода денежных средств без открытия банковских счетов, в том числе электронных денежных средств (за исключением почтовых переводов), на основании несанкционированно модифицированного распоряжения клиента ОПДС	Выявление инцидентов, связанных с осуществлением перевода денежных средств без открытия банковских счетов, в том числе электронных денежных средств (за исключением почтовых переводов), на основании несанкционированно модифицированного распоряжения клиента ОПДС, которые фиксируются кредитной организацией в базе данных о событиях операционного риска и потерях, понесенных вследствие его реализации, в соответствии с п. 1.2 Положения 716-П	Нет требования к бизнес-данным инцидента защиты информации

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
							[MTR_OPDS_4]	Инцидент, связанный с осуществлением перевода денежных средств без открытия банковских счетов, в том числе электронных денежных средств (за исключением почтовых переводов), с искаженными реквизитами в результате НСД к объектам информационной инфраструктуры ОПДС	Выявление инцидентов, связанных с осуществлением переводов денежных средств без открытия банковских счетов, в том числе электронных денежных средств (за исключением почтовых переводов), с искаженными реквизитами в результате НСД к объектам информационной инфраструктуры ОПДС, которые фиксируются кредитной организацией в базе данных о событиях операционного риска и потерях, понесенных вследствие его реализации, в соответствии с п. 1.2 Положения 716-П	Нет требования к бизнес-данным инцидента защиты информации
						[DT_MTR]	[DT_MTR_OPDS_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением)	Выявление факта превышения допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением)	-

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
							[DT_MTR_OPDS_3]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением), а также допустимого времени простоя и (или) деградации технологического процесса, установленного кредитной организацией (сигнальным значением), не превышающего 2 часов для банков, размер активов которых составляет более 500 миллиардов рублей и более или признанных значимыми на рынке платежных услуг, 4 часов для банков с универсальной лицензией, размер активов которого составляет менее 500 миллиардов рублей, 6 часов для банков с базовой лицензией и небанковских кредитных организаций	Выявление факта превышения допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением), а также допустимого времени простоя и (или) деградации технологического процесса, установленного кредитной организацией (сигнальным значением), не превышающего 2 часов для банков, размер активов которых составляет более 500 миллиардов рублей и более или признанных значимыми на рынке платежных услуг, 4 часов для банков с универсальной лицензией, размер активов которого составляет менее 500 миллиардов рублей, 6 часов для банков с базовой лицензией и небанковских кредитных организаций	-
				[operationIn-FinancialMarket]	Технологический процесс, обеспечивающий выполнение операций на финансовых рынках	[DT_BAC]	[DT_BAC_BANK_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением)	Выявление факта превышения допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением)	-

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
							[DT_BAC_BANK_6]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением), а также допустимого времени простоя и (или) деградации технологического процесса, установленного кредитной организацией (сигнальным значением), не превышающего 24 часов (за исключение небанковских кредитных организаций)	Выявление факта превышения допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением), а также допустимого времени простоя и (или) деградации технологического процесса, установленного кредитной организацией (сигнальным значением), не превышающего 24 часов (за исключение небанковских кредитных организаций)	-
				[cashOperation]	Технологический процесс, обеспечивающий выполнение кассовых операций	[BAC]	[BAC_BANK_1]	Инцидент, связанный с несанкционированной выдачей наличных денежных средств кредитной организацией	Выявление событий, связанных с несанкционированной выдачей наличных денежных средств кредитной организацией, которые фиксируются в базе данных о событиях операционного риска и потерях, понесенных вследствие его реализации, в соответствии с п. 1.2 Положения 716-П	Нет требования к бизнес-данным инцидента защиты информации
							[BAC_BANK_2]	Инцидент, связанный с несанкционированным зачислением денежных средств	Выявление событий, связанных с несанкционированным зачислением денежных средств на счет путем приема наличных денежных средств кредитной организацией, которые фиксируются в базе данных о событиях операционного риска и потерях, понесенных вследствие его реализации, в соответствии с п. 1.2 Положения 716-П	Нет требования к бизнес-данным инцидента защиты информации

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
						[DT_BAC]	[DT_BAC_BANK_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением)	Выявление факта превышения допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением)	-
							[DT_BAC_BANK_4]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением), а также допустимого времени простоя и (или) деградации технологического процесса, установленного кредитной организацией (сигнальным значением), не превышающего 2 часов (за исключение небанковских кредитных организаций)	Выявление факта превышения допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением), а также допустимого времени простоя и (или) деградации технологического процесса, установленного кредитной организацией (сигнальным значением), не превышающего 2 часов (за исключение небанковских кредитных организаций)	-
				[onlineServices]	Технологический процесс, обеспечивающий работу онлайн-сервисов дистанционного обслуживания и доступа к осуществлению операций	[DT_BAC]	[DT_BAC_BANK_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением)	Выявление факта превышения допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением)	-

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
							[DT_BAC_BANK_4]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением), а также допустимого времени простоя и (или) деградации технологического процесса, установленного кредитной организацией (сигнальным значением), не превышающего 2 часов (за исключение небанковских кредитных организаций)	Выявление факта превышения допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением), а также допустимого времени простоя и (или) деградации технологического процесса, установленного кредитной организацией (сигнальным значением), не превышающего 2 часов (за исключение небанковских кредитных организаций)	-
				[placementBPD]	Технологический процесс, обеспечивающий размещение и обновление биометрических персональных данных в единой биометрической системе	[BAC]	[BAC_BANK_5]	Инцидент, связанный с нарушением целостности (подмены, удаления) или нарушением достоверности (внесения фиктивных биометрических персональных данных) биометрических персональных данных	Выявление кредитной организацией факта нарушения целостности (подмены, удаления) или нарушения достоверности (внесения фиктивных биометрических персональных данных) биометрических персональных данных	Нет требования к бизнес-данным инцидента защиты информации
						[DT_BAC]	[DT_BAC_BANK_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением)	Выявление факта превышения допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением)	-

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
							[DT_BAC_BANK_4]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением), а также допустимого времени простоя и (или) деградации технологического процесса, установленного кредитной организацией (сигнальным значением), не превышающего 2 часов (за исключение небанковских кредитных организаций)	Выявление факта превышения допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением), а также допустимого времени простоя и (или) деградации технологического процесса, установленного кредитной организацией (сигнальным значением), не превышающего 2 часов (за исключение небанковских кредитных организаций)	-
				[usageBPDforIA]	Технологический процесс, обеспечивающий идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, в том числе с применением информационных технологий без их личного присутствия	[BAC]	[BAC_BANK_6]	Инцидент, связанный с ложноположительной идентификацией и (или) аутентификацией с использованием биометрических персональных данных физических лиц, в том числе с применением информационных технологий без их личного присутствия	Выявление кредитной организацией факта ложноположительной идентификации и (или) аутентификации с использованием биометрических персональных данных физических лиц, в том числе с применением информационных технологий без их личного присутствия	Нет требования к бизнес-данным инцидента защиты информации
							[BAC_BANK_7]	Инцидент, связанный с идентификацией и (или) аутентификацией с использованием биометрических персональных данных физических лиц, в том числе с применением информационных технологий без их личного присутствия, при подмене физическим лицом биометрических персональных данных	Выявление кредитной организацией факта идентификации и (или) аутентификации с использованием биометрических персональных данных физических лиц, в том числе с применением информационных технологий без их личного присутствия, при подмене физическим лицом биометрических персональных данных	Нет требования к бизнес-данным инцидента защиты информации

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
						[DT_BAC]	[DT_BAC_BANK_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением)	Выявление факта превышения допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением)	-
							[DT_BAC_BANK_4]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением), а также допустимого времени простоя и (или) деградации технологического процесса, установленного кредитной организацией (сигнальным значением), не превышающего 2 часов (за исключение небанковских кредитных организаций)	Выявление факта превышения допустимой доли деградации технологического процесса, установленной кредитной организацией (сигнальным значением), а также допустимого времени простоя и (или) деградации технологического процесса, установленного кредитной организацией (сигнальным значением), не превышающего 2 часов (за исключение небанковских кредитных организаций)	-
[OPDS]	Оператор по переводу денежных средств			Технологические процессы ОПДС входят в состав технологических процессов кредитных организаций						-
[OEDS]	Оператор электронных денежных средств			Технологические процессы ОЭДС входят в состав технологических процессов кредитных организаций						-
[OUPI]	Оператор услуг платежной инфраструктуры	[OC]	Операционный центр	[providingMessaging]	Обеспечение обмена ЭС при взаимодействии с ОПДС, клиента ОПДС, ОУИО, ОУПИ (ПКЦ, РЦ)	[MTR]	[MTR_OC_1]	Инцидент, связанный с осуществлением перевода денежных средств с искаженными реквизитами на основании несанкционированно модифицированного ЭС ОПДС, клиента ОПДС, ОУПИ при обеспечении обмена ЭС	Получение ОУПИ (ОЦ) уведомлений в предусмотренной договором форме от ОПДС или самостоятельное выявление факта осуществления перевода денежных средств с искаженными реквизитами на основании несанкционированно модифицированного ЭС ОПДС, клиента ОПДС, ОУПИ при обеспечении обмена ЭС	Нет требования к бизнес-данным инцидента защиты информации

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
							[MTR_OC_2]	Инцидент, связанный с осуществлением перевода денежных средств с искаженными реквизитами в результате НСД к объектам информационной инфраструктуры ОУПИ (ОЦ) при обеспечении обмена ЭС	Получение ОУПИ (ОЦ) уведомлений в предусмотренной договором форме от ОПДС или самостоятельное выявление факта осуществления перевода денежных средств с искаженными реквизитами в результате НСД к объектам информационной инфраструктуры ОУПИ (ОПКЦ) при обеспечении обмена ЭС	Нет требования к бизнес-данным инцидента защиты информации
		[РКС]	Платежный клиринговый центр	[acceptanceForExecution]	Выполнение процедур приема к исполнению ЭС ОПДС, ОУПИ (ОЦ), ОУИО	[MTR]	[MTR_ОРКС_3]	Инцидент, связанный с осуществлением перевода денежных средств с искаженными реквизитами на основании несанкционированно модифицированного ЭС при выполнении процедур приема к исполнению ЭС	Получение ОУПИ (ПКЦ) уведомлений в предусмотренной договором форме или самостоятельное выявление факта осуществления перевода денежных средств с искаженными реквизитами на основании несанкционированно модифицированного ЭС ОПДС, клиента ОПДС, ОУПИ (ОЦ) при выполнении процедур приема к исполнению ЭС	Нет требования к бизнес-данным инцидента защиты информации
							[MTR_ОРКС_4]	Инцидент, связанный с осуществлением перевода денежных средств с искаженными реквизитами в результате НСД к объектам информационной инфраструктуры ОУПИ (ПКЦ) при выполнении процедур приема к исполнению ЭС	Получение ОУПИ (ПКЦ) уведомлений в предусмотренной договором форме или самостоятельное выявление факта осуществления перевода денежных средств с искаженными реквизитами в результате НСД к объектам информационной инфраструктуры ОУПИ (ПКЦ) при выполнении процедур приема к исполнению ЭС	Нет требования к бизнес-данным инцидента защиты информации

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
				[determinationOfPCP]	Определение платежных клиринговых позиций для исполнения принятых ЭС	[MTR]	[MTR_ ОРКС_5]	Инцидент, связанный с осуществлением операции по банковским (корреспондентским) счетам ОПДС с искаженными реквизитами на основании несанкционированно модифицированного ЭС ОПДС, ОУПИ (ОЦ), ОУИО при формировании ЭС для исполнения ОУПИ (РЦ)	Получение ОУПИ (ПКЦ) уведомлений в предусмотренной договором форме или самостоятельное выявление факта осуществления операции по банковским (корреспондентским) счетам ОПДС с искаженными реквизитами на основании несанкционированно модифицированного ЭС ОПДС, ОУПИ (ОЦ), ОУИО при формировании ЭС для исполнения ОУПИ (РЦ)	Нет требования к бизнес-данным инцидента защиты информации
							[MTR_ ОРКС_6]	Инцидент, связанный с осуществлением операции по банковским (корреспондентским) счетам ОПДС с искаженными реквизитами в результате НСД к объектам информационной инфраструктуры ОУПИ (ПКЦ) при формировании ЭС для исполнения ОУПИ (РЦ)	Получение ОУПИ (ПКЦ) уведомлений в предусмотренной договором форме или самостоятельное выявление факта осуществления операции по банковским (корреспондентским) счетам ОПДС с искаженными реквизитами в результате НСД к объектам информационной инфраструктуры ОУПИ (ПКЦ) при формировании ЭС для исполнения ОУПИ (РЦ)	Нет требования к бизнес-данным инцидента защиты информации
							[MTR_ ОРКС_7]	Инцидент, связанный с осуществлением операции по банковским (корреспондентским) счетам ОПДС с искаженными реквизитами на основании несанкционированно модифицированного ЭС ОПДС, ОУПИ (ОЦ), ОУИО при направлении извещений ОПДС	Получение ОУПИ (ПКЦ) уведомлений в предусмотренной договором форме или самостоятельное выявление факта осуществления операции по банковским (корреспондентским) счетам ОПДС с искаженными реквизитами на основании несанкционированно модифицированного ЭС ОПДС, ОУПИ (ОЦ), ОУИО при направлении извещений ОПДС	Нет требования к бизнес-данным инцидента защиты информации

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
							[MTR_OPKC_8]	Инцидент, связанный с осуществлением операции по банковским (корреспондентским) счетам ОПДС с искаженными реквизитами в результате НСД к объектам информационной инфраструктуры ОУПИ (ПКЦ) при направлении извещений ОПДС	Получение ОУПИ (ПКЦ) уведомлений в предусмотренной договором форме или самостоятельное выявление факта осуществления операции по банковским (корреспондентским) счетам ОПДС с искаженными реквизитами в результате НСД к объектам информационной инфраструктуры ОУПИ (ПКЦ) при направлении извещений ОПДС	Нет требования к бизнес-данным инцидента защиты информации
		[RC]	Расчетный центр	[executionOfOrder]	Исполнение поступивших от ОУПИ (ПКЦ) ЭС при списании и зачислении денежных средств по корреспондентским счетам ОПДС	[MTR]	[MTR_RC_1]	Инцидент, связанный с осуществлением операции по банковским (корреспондентским) счетам ОПДС на основании несанкционированно модифицированного ЭС ОУПИ (ПКЦ)	Получение ОУПИ (РЦ) уведомлений в предусмотренной договором форме или самостоятельное выявление факта осуществления операции по банковским (корреспондентским) счетам ОПДС на основании несанкционированно модифицированного ЭС ОУПИ (ПКЦ)	Нет требования к бизнес-данным инцидента защиты информации
							[MTR_RC_2]	Инцидент, связанный с осуществлением операции по банковским (корреспондентским) счетам ОПДС с искаженными реквизитами в результате НСД к объектам информационной инфраструктуры ОУПИ (РЦ)	Получение ОУПИ (РЦ) уведомлений в предусмотренной договором форме или самостоятельное выявление факта осуществления операции по банковским (корреспондентским) счетам ОПДС с искаженными реквизитами в результате НСД к объектам информационной инфраструктуры ОУПИ (РЦ)	Нет требования к бизнес-данным инцидента защиты информации
[OUIO]	Оператор услуг информационного обмена			Нет требования по информированию об инцидентах						
[OPS]	Оператор платежной системы			Нет требования по информированию об инцидентах						
[BPA]	Банковский платежный агент	-		Нет требования по информированию об инцидентах						
		[BPS]	Банковский платежный субагент	Нет требования по информированию об инцидентах						

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
[PA]	Платежный агрегатор			Нет требования по информированию об инцидентах						
[PCB]	Осуществление деятельности профессиональных участников рынка ценных бумаг	[PCB_BRO]	Осуществление брокерской деятельности	[refundOfFunds]	Технологический процесс, обеспечивающий возврат клиентам денежных средств	[FM]	[FM_PCB_BRO_1]	Инцидент, связанный с возвратом клиентам денежных средств на основании требования клиента, сформированного без его согласия, в том числе на основании модифицированного требования клиента	Получение уведомления от клиента или самостоятельное выявление брокером факта перевода денежных средств на основании требования клиента, сформированного без его согласия, в том числе на основании модифицированного требования клиента	Хеш ДУЛ или ИНН клиента (пострадавшей стороны)
										Идентификатор распоряжения на осуществление перевода денежных средств
										ИНН кредитной организации, в которую направлено распоряжение
										N° счета получателя в кредитной организации
										ИНН кредитной организации получателя
							[FM_PCB_BRO_2]	Инцидент, связанный с возвратом клиентам денежных средств в результате НСД к инфраструктуре брокера или инфраструктуре взаимодействия брокера и кредитной организации	Получение уведомления от клиента или самостоятельное выявление брокером факта перевода денежных средств в результате НСД к инфраструктуре брокера или инфраструктуре взаимодействия брокера и кредитной организации	Хеш ДУЛ или ИНН клиента (пострадавшей стороны)
										Идентификатор распоряжения на осуществление перевода денежных средств

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
										ИНН кредитной организации, в которую направлено распоряжение
										N° счета получателя в кредитной организации
										ИНН кредитной организации получателя
						[DT_FS]	[DT_FS_PCB_BRO_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – брокером	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – брокером	-
							[DT_FS_PCB_BRO_2]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – брокером, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – брокером, не превышающего 24 часов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – брокером, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – брокером, не превышающего 24 часов	-
				[executionOfOrders]	Технологический процесс, обеспечивающий исполнение поручений клиентов на совершение сделок с ценными бумагами и заключение договоров, являющихся производными финансовыми инструментами	[FM]	[FM_PCB_BRO_3]	Инцидент, связанный с исполнением поручения клиента на совершение сделки, сформированного без его согласия, в том числе на основании модифицированного поручения клиента	Получение уведомления от клиента или самостоятельное выявление брокером факта исполнения поручения клиента на совершение сделки, сформированного без его согласия, в том числе на основании модифицированного поручения клиента	Собственный код участника торгов

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
										Код клиента участника торгов (пострадавшей стороны)
										Хеш ДУЛ или ИНН клиента (пострадавшей стороны)
										Идентификатор заявки, направленной организатору торговли
										ИНН организатора торговли
										Хеш ДУЛ или ИНН клиента (второй стороны по внебиржевой сделке)
										Идентификатор внебиржевого договора
							[FM_PCB_BRO_4]	Инцидент, связанный с исполнением поручения клиента на совершение сделки в результате НСД к инфраструктуре брокера или инфраструктуре взаимодействия брокера и организатора торговли	Получение уведомления от клиента или самостоятельное выявление брокером факта исполнения поручения клиента на совершение сделки в результате НСД к инфраструктуре брокера или инфраструктуре взаимодействия брокера и организатора торговли	Собственный код участника торгов
										Код клиента участника торгов (пострадавшей стороны)
										Хеш ДУЛ или ИНН клиента (пострадавшей стороны)

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
										Идентификатор заявки, направленной организатору торговли
										ИНН организатора торговли
										Хеш ДУЛ или ИНН клиента (второй стороны по внебиржевой сделке)
										Идентификатор внебиржевого договора
						[DT_FS]	[DT_FS_PCB_BRO_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – брокером	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – брокером	-
							[DT_FS_PCB_BRO_3]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – брокером, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – брокером, не превышающего 2 часов для организаций, обязанных соблюдать усиленный или стандартный уровень защиты информации, 4 часов для иных организаций	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – брокером, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – брокером, не превышающего 2 часов для организаций, обязанных соблюдать усиленный или стандартный уровень защиты информации, 4 часов для иных организаций	-

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
				[accounting-OfOperation]	Технологический процесс, обеспечивающий внесение записей во внутренний учет	[FM]	[FM_PCB_BRO_5]	Инцидент, связанный с внесением записей во внутренний учет в результате НСД к инфраструктуре брокера	Выявление брокером факта внесения записей во внутренний учет в результате НСД к инфраструктуре брокера	Нет требования к бизнес-данным инцидента защиты информации
						[DT_FS]	[DT_FS_PCB_BRO_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – брокером	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – брокером	-
							[DT_FS_PCB_BRO_4]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – брокером, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – брокером, не превышающего 12 часов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – брокером, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – брокером, не превышающего 12 часов	-

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
		[PCB_DIL]	Осуществление дилерской деятельности	[performanceOfDeals]	Технологический процесс, обеспечивающий совершение сделок купли-продажи ценных бумаг от своего имени и за свой счет путем публичного объявления цен покупки и (или) продажи определенных ценных бумаг с обязательством покупки и (или) продажи этих ценных бумаг по объявленным лицом, осуществляющим указанную деятельность, ценам	[FM]	[FM_PCB_DIL_1]	Инцидент, связанный с совершением сделки купли-продажи ценных бумаг в результате НСД к инфраструктуре дилера	Выявление дилером факта совершения сделки купли-продажи ценных бумаг в результате НСД к инфраструктуре дилера	Нет требования к бизнес-данным инцидента защиты информации
						[DT_FS]	[DT_FS_PCB_BRO_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – дилером	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – дилером	-
							[DT_FS_PCB_DIL_2]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – дилером, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – дилером, не превышающего 24 часов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – дилером, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – дилером, не превышающего 24 часов	-

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
				[accounting-OfOperation]	Технологический процесс, обеспечивающий внесение записей во внутренний учет	[FM]	[FM_PCB_DIL_2]	Инцидент, связанный с внесением записей во внутренний учет в результате НСД к инфраструктуре дилера	Выявление дилером факта внесения записей во внутренний учет в результате НСД к инфраструктуре дилера	Нет требования к бизнес-данным инцидента защиты информации
						[DT_FS]	[DT_FS_PCB_BRO_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – дилером	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – дилером	-
							[DT_FS_PCB_DIL_3]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – дилером, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – дилером, не превышающего 12 часов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – дилером, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – дилером, не превышающего 12 часов	-

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
		[PCB_FDIL]	Осуществление деятельности форекс-дилера	[performanceOfDeals]	Технологический процесс, обеспечивающий заключение от своего имени и за свой счет с физическими лицами, не являющимися индивидуальными предпринимателями, не на организованных торгах договоров, указанных в пункте 1 статьи 41 Федерального закона от 22 апреля 1996 года N° 39-ФЗ «О рынке ценных бумаг»	[FM]	[FM_PCB_FDIL_1]	Инцидент, связанный с заключением от своего имени и за свой счет сделки в результате НСД к инфраструктуре форекс-дилера	Выявление дилером факта заключения от своего имени и за свой счет сделки в результате НСД к инфраструктуре форекс-дилера	Нет требования к бизнес-данным инцидента защиты информации
						[DT_FS]	[DT_FS_PCB_FDIL_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – форекс-дилером	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – форекс-дилером	-
							[DT_FS_PCB_FDIL_2]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – форекс-дилером, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – форекс-дилером, не превышающего 2 часов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – форекс-дилером, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – форекс-дилером, не превышающего 2 часов	-

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
				[refundOfFunds]	Технологический процесс, обеспечивающий возврат клиентам денежных средств	[FM]	[FM_PCB_FDIL_2]	Инцидент, связанный с возвратом клиентам денежных средств на основании требования клиента, сформированного без его согласия, в том числе на основании модифицированного требования клиента	Получение уведомления от клиента или самостоятельное выявление форекс-дилером факта перевода денежных средств на основании требования клиента, сформированного без его согласия, в том числе на основании модифицированного требования клиента	Хеш ДУЛ или ИНН клиента (пострадавшей стороны)
										Идентификатор распоряжения на осуществление перевода денежных средств
										ИНН кредитной организации, в которую направлено распоряжение
										N° счета получателя в кредитной организации
										ИНН кредитной организации получателя
							[FM_PCB_FDIL_3]	Инцидент, связанный с возвратом клиентам денежных средств в результате НСД к инфраструктуре форекс-дилера или инфраструктуре взаимодействия форекс-дилера и кредитной организации	Получение уведомления от клиента или самостоятельное выявление форекс-дилером факта перевода денежных средств в результате НСД к инфраструктуре форекс-дилера или инфраструктуре взаимодействия форекс-дилера и кредитной организации	Хеш ДУЛ или ИНН клиента (пострадавшей стороны)
										Идентификатор распоряжения на осуществление перевода денежных средств

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
										ИНН кредитной организации, в которую направлено распоряжение
										N° счета получателя в кредитной организации
										ИНН кредитной организации получателя
						[DT_FS]	[DT_FS_PCB_FDIL_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – форекс-дилером	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – форекс-дилером	-
							[DT_FS_PCB_FDIL_3]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – форекс-дилером, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – форекс-дилером, не превышающего 24 часов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – форекс-дилером, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – форекс-дилером, не превышающего 24 часов	-
				[accounting-OfOperation]	Технологический процесс, обеспечивающий внесение записей во внутренний учет	[FM]	[FM_PCB_FDIL_4]	Инцидент, связанный с внесением записей во внутренний учет в результате НСД к инфраструктуре форекс-дилера	Выявление форекс-дилером факта внесения записей во внутренний учет в результате НСД к инфраструктуре форекс-дилера	Нет требования к бизнес-данным инцидента защиты информации
						[DT_FS]	[DT_FS_PCB_FDIL_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – форекс-дилером	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – форекс-дилером	-

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
							[DT_FS_PCB_FDIL_4]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – форекс-дилером, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – форекс-дилером, не превышающего 12 часов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – форекс-дилером, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – форекс-дилером, не превышающего 12 часов	-
		[PCB_UCB]	Осуществление деятельности по управлению ценными бумагами	[performanceOfDeals]	Технологический процесс, обеспечивающий совершение сделок с ценными бумагами и (или) заключение договоров, являющихся производными финансовыми инструментами, в интересах учредителя управления	[FM]	[FM_PCB_UCB_1]	Инцидент, связанный с совершением сделки с ценными бумагами и (или) заключения договора, являющегося производным финансовым инструментом, в результате НСД к инфраструктуре дилера	Выявление дилером факта совершения сделки с ценными бумагами и (или) заключения договора, являющегося производным финансовым инструментом, в результате НСД к инфраструктуре дилера	Собственный код участника торгов
										Идентификатор заявки, направленной организатору торговли
										ИНН организатора торговли
										Хеш ДУЛ или ИНН клиента (второй стороны по внебиржевой сделке)
										Идентификатор внебиржевого договора

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
						[DT_FS]	[DT_FS_PCB_UCB_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – управляющим	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – управляющим	-
							[DT_FS_PCB_UCB_2]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – управляющим, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – управляющим, не превышающего 4 часов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – управляющим, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – управляющим, не превышающего 4 часов	-
				[refundOfFunds]	Технологический процесс, обеспечивающий возврат клиентам денежных средств	[FM]	[FM_PCB_UCB_2]	Инцидент, связанный с возвратом клиентам денежных средств на основании требования клиента, сформированного без его согласия, в том числе на основании модифицированного требования клиента	Получение уведомления от клиента или самостоятельное выявление управляющим факта перевода денежных средств на основании требования клиента, сформированного без его согласия, в том числе на основании модифицированного требования клиента	Хеш ДУЛ или ИНН клиента (пострадавшей стороны)
										Идентификатор распоряжения на осуществление перевода денежных средств
										ИНН кредитной организации, в которую направлено распоряжение
										N° счета получателя в кредитной организации

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
										ИНН кредитной организации получателя
							[FM_PCB_UCB_3]	Инцидент, связанный с возвратом клиентам денежных средств в результате НСД к инфраструктуре управляющего или инфраструктуре взаимодействия управляющего и кредитной организации	Получение уведомления от клиента или самостоятельное выявление управляющим факта перевода денежных средств в результате НСД к инфраструктуре управляющего или инфраструктуре взаимодействия управляющего и кредитной организации	Хеш ДУЛ или ИНН клиента (пострадавшей стороны)
										Идентификатор распоряжения на осуществление перевода денежных средств
										ИНН кредитной организации, в которую направлено распоряжение
										N° счета получателя в кредитной организации
										ИНН кредитной организации получателя
						[DT_FS]	[DT_FS_PCB_UCB_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – управляющим	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – управляющим	-

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
							[DT_FS_PCB_UCB_3]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – управляющим, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – управляющим, не превышающего 24 часов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – управляющим, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – управляющим, не превышающего 24 часов	-
				[accounting-OfOperation]	Технологический процесс, обеспечивающий внесение записей во внутренний учет	[FM]	[FM_PCB_UCB_4]	Инцидент, связанный с внесением записей во внутренний учет в результате НСД к инфраструктуре управляющего	Выявление управляющим факта внесения записей во внутренний учет в результате НСД к инфраструктуре управляющего	Нет требования к бизнес-данным инцидента защиты информации
						[DT_FS]	[DT_FS_PCB_UCB_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – управляющим	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – управляющим	-
							[DT_FS_PCB_UCB_4]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – управляющим, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – управляющим, не превышающего 12 часов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – управляющим, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – управляющим, не превышающего 12 часов	-
		[PCB_RVC]	Осуществление деятельности регистратора	[accounting-OfOperation]	Технологический процесс, обеспечивающий внесение учетных записей в реестр владельцев ценных бумаг	[FM]	[FM_PCB_RVC_1]	Инцидент, связанный с внесением учетных записей в реестр владельцев ценных бумаг в результате НСД к инфраструктуре регистратора	Выявление регистратором факта внесения учетных записей в реестр владельцев ценных бумаг в результате НСД к инфраструктуре регистратора	Нет требования к бизнес-данным инцидента защиты информации

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
						[DT_FS]	[DT_FS_PCB_RVC_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – регистратором	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – регистратором	-
							[DT_FS_PCB_RVC_2]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – регистратором, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – регистратором, не превышающего 24 часов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – регистратором, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – регистратором, не превышающего 24 часов	-
				[checkOfRights]	Технологический процесс, обеспечивающий осуществление регистратором сверки учитываемых регистратором прав на ценные бумаги с центральным депозитарием по счету номинального держателя центрального депозитария	[DT_FS]	[DT_FS_PCB_RVC_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – регистратором	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – регистратором	-

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
							[DT_FS_PCB_RVC_3]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – регистратором, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – регистратором, не превышающего 4 часов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – регистратором, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – регистратором, не превышающего 4 часов	-
		[PCB_DEP]	Депозитарная деятельность, включая деятельность центрального депозитария	[accounting-OfOperation]	Технологический процесс, обеспечивающий внесение учетных записей в учетные регистры	[FM]	[FM_PCB_DEP_1]	Инцидент, связанный с внесением учетных записей в учетные регистры в результате НСД к инфраструктуре регистратора	Выявление депозитарием факта внесения учетных записей в учетные регистры в результате НСД к инфраструктуре регистратора	Нет требования к бизнес-данным инцидента защиты информации
						[DT_FS]	[DT_FS_PCB_DEP_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – депозитарием	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – депозитарием	-
							[DT_FS_PCB_DEP_2]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – депозитарием, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – депозитарием, не превышающего 24 часов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – депозитарием, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – депозитарием, не превышающего 24 часов	-

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
				[settlementOfDeals]	Технологический процесс, обеспечивающий осуществление расчетным депозитарием расчетов по результатам сделок, совершенных на организованных торгах	[FM]	[FM_PCB_DEP_2]	Инцидент, связанный с осуществлением расчетов по результатам сделок, совершенных на организованных торгах, на основании модифицированного поручения о движении ценных бумаг, направленного клиринговой организацией	Получение уведомления от клиринговой организации или самостоятельное выявление расчетным депозитарием факта осуществления расчетов по результатам сделок, совершенных на организованных торгах, на основании модифицированного поручения о движении ценных бумаг, направленного клиринговой организацией	Идентификатор поручения о движении ценных бумаг, направленного в депозитарий по итогам расчетов и содержащего модифицированную информацию о сделке
										ИНН депозитария/спец. депозитария, в который было направлено поручение
										Хеш ДУЛ или ИНН клиента (получателя)
										N° счета депо получателя
										ИНН депозитария/спец. депозитария получателя
							[FM_PCB_DEP_3]	Инцидент, связанный с осуществлением расчетов по результатам сделок, совершенных на организованных торгах, в результате НСД к инфраструктуре расчетного депозитария	Выявление расчетным депозитарием факта осуществления расчетов по результатам сделок, совершенных на организованных торгах, в результате НСД к инфраструктуре расчетного депозитария	Идентификатор поручения о движении ценных бумаг, направленного в депозитарий по итогам расчетов и содержащего модифицированную информацию о сделке
										ИНН депозитария/спец. депозитария, в который было направлено поручение

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
										Хеш ДУЛ или ИНН клиента (получателя)
										N° счета депо получателя
										ИНН депозитария/спец. депозитария получателя
						[DT_FS]	[DT_FS_PCB_DEP_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – депозитарием	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – депозитарием	-
							[DT_FS_PCB_DEP_3]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – депозитарием, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – депозитарием, не превышающего 2 часов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – депозитарием, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – депозитарием, не превышающего 2 часов	-
				[paymentOfDividends]	Технологический процесс, обеспечивающий выплату депоненту доходов в денежной форме по ценным бумагам, учет прав на которые осуществляет депозитарий, и иных причитающихся владельцам указанных ценных бумаг денежных выплат	[FM]	[FM_PCB_DEP_4]	Инцидент, связанный с выплатой депоненту доходов в денежной форме в результате НСД к инфраструктуре депозитария или инфраструктуре взаимодействия депозитария и кредитной организации	Получение уведомления от депонента или самостоятельное выявление депозитарием факта выплаты депоненту доходов в денежной форме в результате НСД к инфраструктуре депозитария или инфраструктуре взаимодействия депозитария и кредитной организации	Хеш ДУЛ или ИНН клиента (пострадавшей стороны)

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
										Идентификатор распоряжения на осуществление перевода денежных средств
										ИНН кредитной организации, в которую направлено распоряжение
										N° счета получателя в кредитной организации
										ИНН кредитной организации получателя
						[DT_FS]	[DT_FS_PCB_DEP_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – депозитарием	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – депозитарием	-
							[DT_FS_PCB_DEP_2]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – депозитарием, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – депозитарием, не превышающего 24 часов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – депозитарием, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – депозитарием, не превышающего 24 часов	-

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
				[checkOfRights]	Технологический процесс, обеспечивающий осуществление центральным депозитарием сверки учитываемых центральным депозитарием прав на ценные бумаги с регистратором по счету номинального держателя центрального депозитария	[DT_FS]	[DT_FS_PCB_DEP_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – депозитарием	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – депозитарием	-
							[DT_FS_PCB_DEP_4]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – центральным депозитарием, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – центральным депозитарием, не превышающего 4 часов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – центральным депозитарием, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – центральным депозитарием, не превышающего 4 часов	-
[TDO]	Осуществление деятельности организатора торговли			[signDeals]	Технологический процесс, обеспечивающий заключение договора между участниками торгов	[FM]	[FM_TDO_1]	Инцидент, связанный с заключением договора между участниками торгов на основании заявки участника торгов, сформированной без его согласия, в том числе на основании модифицированной заявки участника торгов	Получение уведомления от участника торгов или клиринговой организации, а также самостоятельное выявление организатором торговли факта заключения договора между участниками торгов на основании заявки участника торгов, сформированной без его согласия, в том числе на основании модифицированной заявки участника торгов	Код участника торгов (пострадавшей стороны)

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
										Хеш ДУЛ или ИНН участника торгов (пострадавшей стороны)
										Код участника торгов (второй стороны по сделке)
										Хеш ДУЛ или ИНН клиента (второй стороны по сделке)
										Идентификатор сделки
										ИНН клиринговой организации, осуществляющей клиринг по итогам торгов
							[FM_TDO_2]	Инцидент, связанный с заключением договора между участниками торгов или формированием реестра договоров в результате НСД к инфраструктуре организатора торговли	Получение уведомления от участника торгов или клиринговой организации, а также самостоятельное выявление организатором торговли факта заключения договора между участниками торгов или формирования реестра договоров в результате НСД к инфраструктуре организатора торговли	Код участника торгов (пострадавшей стороны)
										Хеш ДУЛ или ИНН участника торгов (пострадавшей стороны)
										Код участника торгов (второй стороны по сделке)

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
										Хеш ДУЛ или ИНН клиента (второй стороны по сделке)
										Идентификатор сделки
										ИНН клиринговой организации, осуществляющей клиринг по итогам торгов
						[DT_FS]	[DT_FS_TDO_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – организатором торговли	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – организатором торговли	-
							[DT_FS_TDO_2]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – организатором торговли, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – организатором торговли, не превышающего 2 часов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – организатором торговли, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – организатором торговли, не превышающего 2 часов	-

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
				[accounting-OfOperation]	Технологический процесс, обеспечивающий ведение реестра участников торгов и их клиентов, реестра заявок, реестра заключенных на организованных торгах договоров, реестра внебиржевых договоров	[FM]	[FM_TDO_3]	Инцидент, связанный с внесением изменений в реестр участников торгов и их клиентов, реестра заявок, реестр заключенных на организованных торгах договоров, реестр внебиржевых договоров в результате НСД к инфраструктуре организатора торговли	Получение уведомления от участника торгов или клиринговой организации, а также самостоятельное выявление организатором торговли факта внесения изменений в реестр участников торгов и их клиентов, реестра заявок, реестр заключенных на организованных торгах договоров, реестр внебиржевых договоров в результате НСД к инфраструктуре организатора торговли	-
						[DT_FS]	[DT_FS_TDO_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – организатором торговли	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – организатором торговли	-
							[DT_FS_TDO_2]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – организатора торговли, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – организатора торговли, не превышающего 2 часов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – организатора торговли, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – организатора торговли, не превышающего 2 часов	-
				[disclosure-OfInformation]	Технологический процесс, обеспечивающий раскрытие и предоставление информации организатором торговли	[DT_FS]	[DT_FS_TDO_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – организатором торговли	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – организатором торговли	-

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
							[DT_FS_TDO_2]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – организатором торговли, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – организатором торговли, не превышающего 2 часов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – организатором торговли, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – организатором торговли, не превышающего 2 часов	-
[CC]	Осуществление клиринговой деятельности и деятельности центрального контрагента			[determination-OfObligations]	Технологический процесс, обеспечивающий определение подлежащих исполнению обязательств	[FM]	[FM_CC_1]	Инцидент, связанный с определением подлежащих исполнению обязательств на основании модифицированного реестра договоров, направленного организатором торговли	Получение уведомления от участника клиринга или организатора торговли, а также самостоятельное выявление клиринговой организацией факта определения подлежащих исполнению обязательств на основании модифицированного реестра договоров, направленного организатором торговли	Нет требования к бизнес-данным инцидента защиты информации
							[FM_CC_2]	Инцидент, связанный с определением подлежащих исполнению обязательств в результате НСД к инфраструктуре клиринговой организации	Получение уведомления от участника клиринга или самостоятельное выявление клиринговой организацией факта определения подлежащих исполнению обязательств в результате НСД к инфраструктуре клиринговой организации	Нет требования к бизнес-данным инцидента защиты информации
						[DT_FS]	[DT_FS_CC_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – клиринговой организацией или центральным контрагентом	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – клиринговой организацией или центральным контрагентом	-

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
							[DT_FS_CC_2]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – клиринговой организацией или центральным контрагентом, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – клиринговой организацией или центральным контрагентом, не превышающего 2 часов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – клиринговой организацией или центральным контрагентом, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – клиринговой организацией или центральным контрагентом, не превышающего 2 часов	-
				[executionOfObligations]	Технологический процесс, обеспечивающий совершение действий, направленных на исполнение подлежащих исполнению обязательств	[FM]	[FM_CC_3]	Инцидент, связанный с совершением действий, направленных на исполнение подлежащих исполнению обязательств, на основании модифицированного реестра договоров, направленного организатором торговли	Получение уведомления от участника клиринга, а также самостоятельное выявление клиринговой организацией факта совершения действий, направленных на исполнение подлежащих исполнению обязательств, на основании модифицированного реестра договоров, направленного организатором торговли	Хеш ДУЛ или ИНН клиента (выгодоприобретателя)

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
										Если направлено распоряжение на осуществление перевода денежных средств: Идентификатор распоряжения на осуществление перевода денежных средств ИНН кредитной организации, в которую направлено распоряжение N° счета получателя в кредитной организации ИНН кредитной организации получателя
										Если направлено поручение о движении ценных бумаг: Идентификатор поручения о движении ценных бумаг ИНН депозитария/спец. депозитария, в который было направлено поручение N° счета депо получателя ИНН депозитария/спец. депозитария получателя

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
							[FM_CC_4]	Инцидент, связанный с совершением действий, направленных на исполнение подлежащих исполнению обязательств, на основании реестра договоров, в результате НСД к инфраструктуре клиринговой организации или инфраструктуре взаимодействия клиринговой организации и расчетной организации, расчетного депозитария	Получение уведомления от участника клиринга, а также самостоятельное выявление клиринговой организацией факта совершения действий, направленных на исполнение подлежащих исполнению обязательств, в результате НСД к инфраструктуре клиринговой организации или инфраструктуре взаимодействия клиринговой организации и расчетной организации, расчетного депозитария	Хеш ДУЛ или ИНН клиента (выгодоприобретателя) Если направлено распоряжение на осуществление перевода денежных средств: Идентификатор распоряжения на осуществление перевода денежных средств ИНН кредитной организации, в которую направлено распоряжение N° счета получателя в кредитной организации ИНН кредитной организации получателя

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
										Если направлено поручение о движении ценных бумаг: Идентификатор поручения о движении ценных бумаг ИНН депозитария/спец. депозитария, в который было направлено поручение N° счета депо получателя ИНН депозитария/спец. депозитария получателя
						[DT_FS]	[DT_FS_CC_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – клиринговой организацией или центральным контрагентом	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – клиринговой организацией или центральным контрагентом	-
							[DT_FS_CC_2]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – клиринговой организацией или центральным контрагентом, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – клиринговой организацией или центральным контрагентом, не превышающего 2 часов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – клиринговой организацией или центральным контрагентом, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – клиринговой организацией или центральным контрагентом, не превышающего 2 часов	-

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
				[refundOfAssets]	Технологический процесс, обеспечивающий направление поручения на возврат имущества, являющегося клиринговым обеспечением	[FM]	[FM_CC_5]	Инцидент, связанный с направлением поручения на возврат имущества, являющегося клиринговым обеспечением, на основании поручения участника клиринга, сформированного без его согласия, в том числе на основании модифицированного поручения	Получение уведомления от участника клиринга или самостоятельное выявление клиринговой организацией факта направления поручения на возврат имущества, являющегося клиринговым обеспечением, на основании поручения участника клиринга, сформированного без его согласия, в том числе на основании модифицированного поручения	Хеш ДУЛ или ИНН клиента (пострадавшей стороны)
										Если направлено распоряжение на осуществление перевода денежных средств: Идентификатор распоряжения на осуществление перевода денежных средств ИНН кредитной организации, в которую направлено распоряжение № счета получателя в кредитной организации ИНН кредитной организации получателя

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
										Если направлено поручение о движении ценных бумаг: Идентификатор поручения о движении ценных бумаг ИНН депозитария/спец. депозитария, в который было направлено поручение N° счета депо получателя ИНН депозитария/спец. депозитария получателя
							[FM_CC_6]	Инцидент, связанный с направлением поручения на возврат имущества, являющегося клиринговым обеспечением, в результате НСД к инфраструктуре клиринговой организации или инфраструктуре взаимодействия клиринговой организации и расчетной организации, расчетного депозитария	Получение уведомления от участника клиринга или самостоятельное выявление клиринговой организацией факта направления поручения на возврат имущества, являющегося клиринговым обеспечением, в результате НСД к инфраструктуре клиринговой организации или инфраструктуре взаимодействия клиринговой организации и расчетной организации, расчетного депозитария	Хеш ДУЛ или ИНН клиента (пострадавшей стороны)

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
										Если направлено распоряжение на осуществление перевода денежных средств: Идентификатор распоряжения на осуществление перевода денежных средств ИНН кредитной организации, в которую направлено распоряжение N° счета получателя в кредитной организации ИНН кредитной организации получателя
										Если направлено поручение о движении ценных бумаг: Идентификатор поручения о движении ценных бумаг ИНН депозитария/спец. депозитария, в который было направлено поручение N° счета депо получателя ИНН депозитария/спец. депозитария получателя

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
						[DT_FS]	[DT_FS_CC_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – клиринговой организацией или центральным контрагентом	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – клиринговой организацией или центральным контрагентом	-
							[DT_FS_CC_2]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – клиринговой организацией или центральным контрагентом, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – клиринговой организацией или центральным контрагентом, не превышающего 2 часов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – клиринговой организацией или центральным контрагентом, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – клиринговой организацией или центральным контрагентом, не превышающего 2 часов	-
[RO]	Осуществление репозитарной деятельности	-	-	[accounting-OTCDeals]	Технологический процесс, обеспечивающий учет заключенных не на организованных торгах договоров репо, договоров, являющихся производными финансовыми инструментами, а также иных договоров	[FM]	[FM_RO_1]	Инцидент, связанный с учетом заключенного не на организованных торгах договоров репо, договора, являющегося производным финансовым инструментом или иного договора, на основании электронного сообщения клиента репозитария, сформированного без его согласия, в том числе на основании модифицированного электронного сообщения клиента репозитария	Получение уведомления от клиента репозитария или самостоятельное выявление репозитарием факта учета заключенного не на организованных торгах договоров репо, договора, являющегося производным финансовым инструментом или иного договора, на основании электронного сообщения клиента репозитария, сформированного без его согласия, в том числе на основании модифицированного электронного сообщения клиента репозитария	Нет требования к бизнес-данным инцидента защиты информации

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
							[FM_RO_2]	Инцидент, связанный с учетом заключенного не на организованных торгах договоров репо, договора, являющегося производным финансовым инструментом или иного договора, в результате НСД к инфраструктуре репозитария	Получение уведомления от клиента репозитария или самостоятельное выявление репозитарием факта учета заключенного не на организованных торгах договоров репо, договора, являющегося производным финансовым инструментом или иного договора, в результате НСД к инфраструктуре репозитария	Нет требования к бизнес-данным инцидента защиты информации
						[DT_FS]	[DT_FS_RO_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – репозитарием	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – репозитарием	-
							[DT_FS_RO_2]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – репозитарием, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – репозитарием, не превышающего 12 часов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – репозитарием, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – репозитарием, не превышающего 12 часов	-
				[transferOfRegistry]	Технологический процесс, обеспечивающий передачу (предоставление) реестра, ведение которого осуществляет репозитарий, в Банк России или в другой репозитарий	[DT_FS]	[DT_FS_RO_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – репозитарием	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – репозитарием	-

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
							[DT_FS_RO_2]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – репозитарием, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – репозитарием, не превышающего 6 часов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – репозитарием, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – репозитарием, не превышающего 6 часов	-
		[RFT]	Регистратор финансовых транзакций	[accounting-OfTransaction]	Технологический процесс, обеспечивающий учет регистратором финансовых транзакций информации о совершении финансовых сделок и об операциях по ним с использованием финансовой платформы	[FM]	[FM_RFT_1]	Инцидент, связанный с учетом совершенных финансовых сделок и операций по ним с использованием финансовой платформы на основании электронного сообщения оператора финансовой платформы, сформированного без его согласия или на основании модифицированного электронного сообщения оператора финансовой платформы	Получение уведомление от оператора финансовой платформы или самостоятельное выявление регистратором финансовых транзакций факта учета совершенной финансовой сделки или операции по ней с использованием финансовой платформы на основании электронного сообщения оператора финансовой платформы, сформированного без его согласия или на основании модифицированного электронного сообщения оператора финансовой платформы	Нет требования к бизнес-данным инцидента защиты информации

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
							[FM_RFT_2]	Инцидент, связанный с учетом совершенных финансовых сделок и операций по ним с использованием финансовой платформы в результате НСД к инфраструктуре регистратора финансовых транзакций или инфраструктуре взаимодействия оператора финансовой платформы и регистратора финансовых транзакций	Получение уведомление от оператора финансовой платформы или самостоятельное выявление регистратором финансовых транзакций факта учета совершенной финансовой сделки или операции по ней с использованием финансовой платформы в результате НСД к инфраструктуре регистратора финансовых транзакций или инфраструктуре взаимодействия оператора финансовой платформы и регистратора финансовых транзакций	Нет требования к бизнес-данным инцидента защиты информации
						[DT_FS]	[DT_FS_RFT_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – регистратором финансовых транзакций	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – регистратором финансовых транзакций	-
							[DT_FS_RFT_2]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – регистратором финансовых транзакций, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – регистратором, не превышающего 2 часов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – регистратором финансовых транзакций, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – регистратором, не превышающего 2 часов	-

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
[UCB]	Осуществление деятельности управляющих компаний инвестиционного фонда, паевого инвестиционного фонда и негосударственного пенсионного фонда			[trustManagement]	Технологический процесс, обеспечивающий доверительное управление имуществом фондов, в том числе осуществление прав, удостоверенных ценными бумагами, составляющими имущество фондов	[FM]	[FM_UCB_1]	Инцидент, связанный с осуществлением операций с имуществом фондов в результате НСД к инфраструктуре управляющей компании	Получение уведомления от специализированного депозитария или фонда, а также самостоятельное выявление управляющей компанией факта осуществления операции с имуществом фонда в результате НСД к инфраструктуре управляющей компании	ИНН фонда (пострадавшей стороны)
										Если направлено распоряжение на осуществление перевода денежных средств: Идентификатор распоряжения на осуществление перевода денежных средств ИНН кредитной организации, в которую направлено распоряжение № счета получателя в кредитной организации ИНН кредитной организации получателя

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
										Если направлено поручение о движении ценных бумаг: Идентификатор поручения о движении ценных бумаг ИНН депозитария/спец. депозитария, в который было направлено поручение N° счета депо получателя ИНН депозитария/спец. депозитария получателя
										Если направлена заявка брокеру: Идентификатор заявки ИНН брокера
						[DT_FS]	[DT_FS_UCB_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – управляющей компанией	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – управляющей компанией	-

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
							[DT_FS_UCB_2]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – управляющей компанией, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – управляющей компанией, не превышающего 2 часов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – управляющей компанией, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – управляющей компанией, не превышающего 2 часов	-
				[exerciseOfRights]	Технологический процесс, обеспечивающий реализацию прав владельцев инвестиционных паев	[FM]	[FM_UCB_2]	Инцидент, связанный с изменением прав владельцев инвестиционных паев в реестре владельцев инвестиционных паев в результате НСД к инфраструктуре управляющей компании	Получение уведомления от специализированного депозитария или фонда, а также самостоятельное выявление управляющей компанией факта изменения прав владельцев инвестиционных паев в реестре владельцев инвестиционных паев в результате НСД к инфраструктуре управляющей компании	-
							[FM_UCB_3]	Инцидент, связанный с погашением инвестиционного пая на основании электронного сообщения владельца инвестиционного пая, сформированного без его согласия или на основании модифицированного электронного сообщения владельца инвестиционного пая	Получение уведомления от специализированного депозитария или фонда, а также самостоятельное выявление управляющей компанией факта погашения инвестиционного пая на основании электронного сообщения владельца инвестиционного пая, сформированного без его согласия или на основании модифицированного электронного сообщения владельца инвестиционного пая	Идентификатор распоряжения на осуществление перевода денежных средств

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
										ИНН кредитной организации, в которую направлено распоряжение
										N° счета получателя в кредитной организации
										ИНН кредитной организации получателя
							[FM_UCB_4]	Инцидент, связанный с погашением инвестиционного пая в результате НСД к инфраструктуре управляющей компании	Получение уведомления от специализированного депозитария или фонда, а также самостоятельное выявление управляющей компанией факта погашения инвестиционного пая в результате НСД к инфраструктуре управляющей компании	Идентификатор распоряжения на осуществление перевода денежных средств
										ИНН кредитной организации, в которую направлено распоряжение
										N° счета получателя в кредитной организации
										ИНН кредитной организации получателя

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
							[FM_UCB_5]	Инцидент, связанный с выплатой денежной компенсации при прекращении договора доверительного управления фондом в результате НСД к инфраструктуре управляющей компании	Получение уведомления от специализированного депозитария или фонда, а также самостоятельное выявление управляющей компанией факта выплаты денежной компенсации при прекращении договора доверительного управления фондом в результате НСД к инфраструктуре управляющей компании	Идентификатор распоряжения на осуществление перевода денежных средств
										ИНН кредитной организации, в которую направлено распоряжение
										N° счета получателя в кредитной организации
										ИНН кредитной организации получателя
						[DT_FS]	[DT_FS_UCB_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – управляющей компанией	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – управляющей компанией	-
							[DT_FS_UCB_3]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – управляющей компанией, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – управляющей компанией, не превышающего 24 часов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – управляющей компанией, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – управляющей компанией, не превышающего 24 часов	-

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
				[accountingOfAssets]	Технологический процесс, обеспечивающий осуществление учета имущества фондов и контроля за распоряжением им, в том числе процесс взаимодействия со специализированным депозитарием	[DT_FS]	[DT_FS_UCB_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – управляющей компанией	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – управляющей компанией	-
							[DT_FS_UCB_3]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – управляющей компанией, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – управляющей компанией, не превышающего 24 часов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – управляющей компанией, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – управляющей компанией, не превышающего 24 часов	-
[SDIF]	Осуществление деятельности специализированных депозитариев инвестиционного фонда, паевого инвестиционного фонда и негосударственного пенсионного фонда			[controlOfOperation]	Технологический процесс, обеспечивающий осуществление специализированным депозитарием контроля за распоряжением имуществом фондов	[FM]	[FM_SDIF_1]	Инцидент, связанный с согласованием нелегитимных заявок, направленных из скомпрометированной инфраструктуры управляющей компании и (или) фондов	Получение уведомления от управляющей компании или фонда, а также самостоятельное выявление специализированным депозитарием факта согласования нелегитимной заявки, направленной из скомпрометированной инфраструктуры управляющей компании и (или) фонда	Нет требования к бизнес-данным инцидента защиты информации

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
						[DT_FS]	[DT_FS_SDIF_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – специализированным депозитарием инвестиционного фонда, паевым инвестиционным фондом и негосударственным пенсионным фондом	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – специализированным депозитарием инвестиционного фонда, паевым инвестиционным фондом и негосударственным пенсионным фондом	-
							[DT_FS_SDIF_2]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – специализированным депозитарием инвестиционного фонда, паевым инвестиционным фондом и негосударственным пенсионным фондом, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – специализированным депозитарием инвестиционного фонда, паевым инвестиционным фондом и негосударственным пенсионным фондом, не превышающего 24 часов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – специализированным депозитарием инвестиционного фонда, паевым инвестиционным фондом и негосударственным пенсионным фондом, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – специализированным депозитарием инвестиционного фонда, паевым инвестиционным фондом и негосударственным пенсионным фондом, не превышающего 24 часов	-

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
				[accountingOfHolders]	Технологический процесс, обеспечивающий внесение учетных записей в реестр владельцев ценных бумаг (в случае оказания услуг по ведению реестра владельцев инвестиционных паев паевых инвестиционных фондов, ипотечных сертификатов участия)	[FM]	[FM_SDIF_2]	Инцидент, связанный с внесением учетных записей в реестр владельцев ценных бумаг в результате НСД к инфраструктуре регистратора	Выявление специализированным депозитарием факта внесения учетных записей в реестр владельцев ценных бумаг в результате НСД к инфраструктуре регистратора	Нет требования к бизнес-данным инцидента защиты информации
						[DT_FS]	[DT_FS_SDIF_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – специализированным депозитарием инвестиционного фонда, паевым инвестиционным фондом и негосударственным пенсионным фондом	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – специализированным депозитарием инвестиционного фонда, паевым инвестиционным фондом и негосударственным пенсионным фондом	-

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
							[DT_FS_SDIF_2]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – специализированным депозитарием инвестиционного фонда, паевым инвестиционным фондом и негосударственным пенсионным фондом, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – специализированным депозитарием инвестиционного фонда, паевым инвестиционным фондом и негосударственным пенсионным фондом, не превышающего 24 часов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – специализированным депозитарием инвестиционного фонда, паевым инвестиционным фондом и негосударственным пенсионным фондом, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – специализированным депозитарием инвестиционного фонда, паевым инвестиционным фондом и негосударственным пенсионным фондом, не превышающего 24 часов	-
[INCIF]	Осуществление деятельности акционерных инвестиционных фондов			Нет требования по информированию об инцидентах						
[NGPF]	Осуществление деятельности негосударственных пенсионных фондов			[payments-ToCustomers]	Технологический процесс, обеспечивающий осуществление выплат вкладчикам, участникам, застрахованным лицам и их правопреемникам негосударственного пенсионного фонда в рамках обязательного пенсионного страхования негосударственного пенсионного обеспечения	[FM]	[FM_NGPF_1]	Инцидент, связанный с осуществлением выплат в рамках обязательного пенсионного страхования и негосударственного пенсионного обеспечения в результате НСД к инфраструктуре НПФ или инфраструктуре взаимодействия НПФ и кредитной организации	Получение уведомления от вкладчика, участника, застрахованного лица, правопреемника или кредитной организации, а также самостоятельное выявление НПФ факта осуществления выплаты в рамках обязательного пенсионного страхования и негосударственного пенсионного обеспечения в результате НСД к инфраструктуре НПФ или инфраструктуре взаимодействия НПФ и кредитной организации	Хеш ДУЛ или ИНН клиента (пострадавшей стороны)

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
										Идентификатор распоряжения на осуществление перевода денежных средств
										ИНН кредитной организации, в которую направлено распоряжение
										N° счета получателя в кредитной организации
										ИНН кредитной организации получателя
						[DT_FS]	[DT_FS_NGPF_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – негосударственным пенсионным фондом	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – негосударственным пенсионным фондом	-
							[DT_FS_NGPF_2]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – негосударственным пенсионным фондом, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – негосударственным пенсионным фондом, не превышающего 24 часов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – негосударственным пенсионным фондом, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – негосударственным пенсионным фондом, не превышающего 24 часов	-

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
				[transferToUCB]	Технологический процесс, обеспечивающий передачу средств пенсионных резервов и пенсионных накоплений управляющей компании	[FM]	[FM_ NGPF_2]	Инцидент, связанный с передачей средств пенсионных резервов и пенсионных накоплений управляющей компании в результате НСД к инфраструктуре НПФ или инфраструктуре взаимодействия НПФ и кредитной организации	Получение уведомления от управляющей компании или кредитной организации, а также самостоятельное выявление НПФ факта передачи средств пенсионных резервов и пенсионных накоплений управляющей компании в результате НСД к инфраструктуре НПФ или инфраструктуре взаимодействия НПФ и кредитной организации	Идентификатор распоряжения на осуществление перевода денежных средств
										ИНН кредитной организации, в которую направлено распоряжение
										N° счета получателя в кредитной организации
										ИНН кредитной организации получателя
						[DT_FS]	[DT_FS_ NGPF_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – негосударственным пенсионным фондом	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – негосударственным пенсионным фондом	-

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
							[DT_FS_NGPF_2]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – негосударственным пенсионным фондом, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – негосударственным пенсионным фондом, не превышающего 24 часов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – негосударственным пенсионным фондом, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – негосударственным пенсионным фондом, не превышающего 24 часов	-
				[transferToNGPF]	Технологический процесс, обеспечивающий перевод выкупных сумм (средств пенсионных накоплений) в иные негосударственные пенсионные фонды и Пенсионный фонд Российской Федерации	[FM]	[FM_NGPF_3]	Инцидент, связанный с переводом выкупных сумм в результате НСД к инфраструктуре НПФ или инфраструктуре взаимодействия НПФ и кредитной организации	Получение уведомления от кредитной организации или самостоятельное выявление НПФ факта перевода выкупной суммы в результате НСД к инфраструктуре НПФ или инфраструктуре взаимодействия НПФ и кредитной организации	Идентификатор распоряжения на осуществление перевода денежных средств
										ИНН кредитной организации, в которую направлено распоряжение
										N° счета получателя в кредитной организации
										ИНН кредитной организации получателя

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
						[DT_FS]	[DT_FS_NGPF_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – негосударственным пенсионным фондом	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – негосударственным пенсионным фондом	-
							[DT_FS_NGPF_2]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – негосударственным пенсионным фондом, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – негосударственным пенсионным фондом, не превышающего 24 часов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – негосударственным пенсионным фондом, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – негосударственным пенсионным фондом, не превышающего 24 часов	-
				[placementOfFunds]	Технологический процесс, обеспечивающий размещение средств пенсионных резервов	[FM]	[FM_NGPF_4]	Инцидент, связанный с размещением средств пенсионных резервов в результате НСД к инфраструктуре НПФ или инфраструктуре взаимодействия НПФ и кредитной организации	Получение уведомления от кредитной организации или самостоятельное выявление НПФ факта размещения средств пенсионных резервов в результате НСД к инфраструктуре НПФ или инфраструктуре взаимодействия НПФ и кредитной организации	Идентификатор распоряжения на осуществление перевода денежных средств
										ИНН кредитной организации, в которую направлено распоряжение
										N° счета получателя в кредитной организации
										ИНН кредитной организации получателя

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
						[DT_FS]	[DT_FS_NGPF_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – негосударственным пенсионным фондом	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – негосударственным пенсионным фондом	-
							[DT_FS_NGPF_2]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – негосударственным пенсионным фондом, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – негосударственным пенсионным фондом, не превышающего 24 часов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – негосударственным пенсионным фондом, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – негосударственным пенсионным фондом, не превышающего 24 часов	-
				[terminationOfAgreement]	Технологический процесс, обеспечивающий расторжение договора негосударственного пенсионного обеспечения, договора об обязательном пенсионном страховании негосударственным пенсионным фондом	[FM]	[FM_NGPF_5]	Инцидент, связанный с осуществлением выплат в связи с расторжением договора на основании заявления клиента НПФ, сформированного без его согласия, в том числе на основании модифицированного заявления	Получение уведомления от клиента НПФ или самостоятельное выявление НПФ факта осуществления выплаты в связи с расторжением договора на основании заявления клиента НПФ, сформированного без его согласия, в том числе на основании модифицированного заявления	Хеш ДУЛ или ИНН клиента (пострадавшей стороны)
										Идентификатор распоряжения на осуществление перевода денежных средств

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
										ИНН кредитной организации, в которую направлено распоряжение
										N° счета получателя в кредитной организации
										ИНН кредитной организации получателя
							[FM_NGPF_6]	Инцидент, связанный с осуществлением выплат в связи с расторжением договора в результате НСД к инфраструктуре НПФ или инфраструктуре взаимодействия НПФ и кредитной организации	Получение уведомления от клиента НПФ или самостоятельное выявление НПФ факта осуществления выплаты в связи с расторжением договора в результате НСД к инфраструктуре НПФ или инфраструктуре взаимодействия НПФ и кредитной организации	Хеш ДУЛ или ИНН клиента (пострадавшей стороны)
										Идентификатор распоряжения на осуществление перевода денежных средств
										ИНН кредитной организации, в которую направлено распоряжение
										N° счета получателя в кредитной организации
										ИНН кредитной организации получателя

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
						[DT_FS]	[DT_FS_NGPF_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – негосударственным пенсионным фондом	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – негосударственным пенсионным фондом	-
							[DT_FS_NGPF_2]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – негосударственным пенсионным фондом, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – негосударственным пенсионным фондом, не превышающего 24 часов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – негосударственным пенсионным фондом, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – негосударственным пенсионным фондом, не превышающего 24 часов	-
[SIB]	Осуществление деятельности субъектов страхового дела			[accounting-OfInsurance]	Технологический процесс, обеспечивающий учет страховых случаев	[FM]	[FM_SIB_1]	Инцидент, связанный с выплатой возмещения на основании заявления клиента, сформированного без его согласия, в том числе на основании модифицированного заявления	Получение уведомления от клиента или самостоятельное выявление субъектом страхового дела факта выплаты возмещения на основании заявления клиента, сформированного без его согласия, в том числе на основании модифицированного заявления	Хеш ДУЛ или ИНН клиента (выгодоприобретателя)
										Идентификатор распоряжения на осуществление перевода денежных средств
										ИНН кредитной организации, в которую направлено распоряжение

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
										N° счета получателя в кредитной организации
										ИНН кредитной организации получателя
							[FM_SIB_2]	Инцидент, связанный с выплатой возмещения в результате НСД к инфраструктуре субъектов страхового дела	Получение уведомления от клиента или самостоятельное выявление субъектом страхового дела факта выплаты возмещения в результате НСД к инфраструктуре субъектов страхового дела	Хеш ДУЛ или ИНН клиента
										Идентификатор распоряжения на осуществление перевода денежных средств
										ИНН кредитной организации, в которую направлено распоряжение
										N° счета получателя в кредитной организации
										ИНН кредитной организации получателя
						[DT_FS]	[DT_FS_SIB_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – страховой организацией	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – страховой организацией	-

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
							[DT_FS_SIB_2]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – страховой организацией, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – страховой организацией, не превышающего 24 часов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – страховой организацией, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – страховой организацией, не превышающего 24 часов	-
				[refundOfInsurance]	Технологический процесс, обеспечивающий возврат страховой премии	[FM]	[FM_SIB_3]	Инцидент, связанный возвратом страховой премии на основании заявления клиента, сформированного без его согласия, в том числе на основании модифицированного заявления	Получение уведомления от клиента или самостоятельное выявление субъектом страхового дела факта возврата страховой премии на основании заявления клиента, сформированного без его согласия, в том числе на основании модифицированного заявления	Хеш ДУЛ или ИНН клиента (выгодоприобретателя)
										Идентификатор распоряжения на осуществление перевода денежных средств
										ИНН кредитной организации, в которую направлено распоряжение
										N° счета получателя в кредитной организации
										ИНН кредитной организации получателя

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
							[FM_SIB_4]	Инцидент, связанный с возвратом страховой премии в результате НСД к инфраструктуре субъектов страхового дела	Получение уведомления от клиента или самостоятельное выявление субъектом страхового дела факта возврата страховой премии в результате НСД к инфраструктуре субъектов страхового дела	Хеш ДУЛ или ИНН клиента
										Идентификатор распоряжения на осуществление перевода денежных средств
										ИНН кредитной организации, в которую направлено распоряжение
										N° счета получателя в кредитной организации
										ИНН кредитной организации получателя
						[DT_FS]	[DT_FS_SIB_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – страховой организацией	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – страховой организацией	-

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
							[DT_FS_SIB_2]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – страховой организацией, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – страховой организацией, не превышающего 24 часов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – страховой организацией, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – страховой организацией, не превышающего 24 часов	-
				[maintenance-OfWebsite]	Технологический процесс, обеспечивающий работу сайтов в части размещения информации, предусмотренной пунктом 6 статьи 6 Закона Российской Федерации от 27 ноября 1992 года № 4015-I «Об организации страхового дела в Российской Федерации»	[DT_FS]	[DT_FS_SIB_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – страховой организацией	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – страховой организацией	-
							[DT_FS_SIB_2]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – страховой организацией, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – страховой организацией, не превышающего 24 часов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – страховой организацией, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – страховой организацией, не превышающего 24 часов	-

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
[MFO]	Осуществление деятельности микрофинансовых организаций			Нет требования по информированию об инцидентах						
[LCC]	Осуществление деятельности кредитных потребительских кооперативов			Нет требования по информированию об инцидентах						
[HCC]	Осуществление деятельности жилищных накопительных кооперативов			Нет требования по информированию об инцидентах						
[AO]	Осуществление актуарной деятельности			Нет требования по информированию об инцидентах						
[CRB]	Осуществление деятельности бюро кредитных историй			[transferOfSubjectCreditHistory]	Передача источником формирования кредитной истории информации о субъекте кредитной истории в БКИ	[FM]	[FM_CRB_1]	Инцидент, связанный с направлением в БКИ информации о субъекте кредитной истории, сформированной без согласия источника формирования кредитной истории, в том числе на основании модифицированной кредитной истории субъекта	Выявление БКИ факта направления в БКИ информации о субъекте кредитной истории, сформированной без согласия источника формирования кредитной истории, в том числе на основании модифицированной кредитной истории субъекта	Нет требования к бизнес-данным инцидента защиты информации
				[transferOfSubject-CreditReport]	Передача БКИ кредитного отчета субъекта пользователям БКИ	[FM]	[FM_ CRB_2]	Инцидент, связанный с передачей БКИ модифицированного кредитного отчета субъекта, в результате НСД к инфраструктуре БКИ	Выявление БКИ факта передачи БКИ модифицированного кредитного отчета субъекта, в результате НСД к инфраструктуре БКИ	Нет требования к бизнес-данным инцидента защиты информации
[CRA]	Осуществление деятельности кредитных рейтинговых агентств			Нет требования по информированию об инцидентах						
[ACCC]	Осуществление деятельности сельскохозяйственных кредитных потребительских кооперативов			Нет требования по информированию об инцидентах						
[PB]	Осуществление деятельности ломбардов			Нет требования по информированию об инцидентах						
[OIP]	Осуществление деятельности оператора инвестиционной платформы			[accessToPlatform]	Технологический процесс, обеспечивающий предоставление доступа к инвестиционной платформе	[DT_FS]	[DT_FS_ OIP_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором инвестиционной платформы	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором инвестиционной платформы	-

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
							[DT_FS_OIP_2]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором инвестиционной платформы, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – оператором инвестиционной платформы, не превышающего 24 часов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором инвестиционной платформы, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – оператором инвестиционной платформы, не превышающего 24 часов	-
				[placement-OfInvestment-Proposal]	Технологический процесс, обеспечивающий размещение инвестиционного предложения	[FM]	[FM_OIP_1]	Инцидент, связанный с размещением инвестиционного предложения на основании поручения лица, привлекающего инвестиции, сформированного без его согласия, в том числе на основании модифицированного поручения лица, привлекающего инвестиции	Получение уведомления от лица, привлекающего инвестиции, или самостоятельное выявление оператором инвестиционной платформы факта размещения инвестиционного предложения на основании поручения лица, привлекающего инвестиции, сформированного без его согласия, в том числе на основании модифицированного поручения лица, привлекающего инвестиции	Нет требования к бизнес-данным инцидента защиты информации
							[FM_OIP_2]	Инцидент, связанный с размещением инвестиционного предложения в результате НСД к информационной инфраструктуре оператора инвестиционной платформы	Получение уведомления от лица, привлекающего инвестиции, или самостоятельное выявление оператором инвестиционной платформы факта размещения инвестиционного предложения в результате НСД к информационной инфраструктуре оператора инвестиционной платформы	Нет требования к бизнес-данным инцидента защиты информации

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
						[DT_FS]	[DT_FS_OIP_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором инвестиционной платформы	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором инвестиционной платформы	-
							[DT_FS_OIP_2]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором инвестиционной платформы, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – оператором инвестиционной платформы, не превышающего 24 часов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором инвестиционной платформы, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – оператором инвестиционной платформы, не превышающего 24 часов	-
				[investmentByLoan]	Технологический процесс, обеспечивающий инвестирование с использованием инвестиционной платформы путем предоставления займов	[FM]	[FM_OIP_3]	Инцидент, связанный с заключением договора инвестирования на основании заявки инвестора, сформированной без его согласия, в том числе на основании модифицированной заявки инвестора	Получение уведомления от инвестора или самостоятельное выявление оператором инвестиционной платформы факта заключения договора инвестирования на основании заявки инвестора, сформированной без его согласия, в том числе на основании модифицированной заявки инвестора	Нет требования к бизнес-данным инцидента защиты информации

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
							[FM_OIP_4]	Инцидент, связанный с заключением договора инвестирования без согласия инвестора в результате НСД к информационной инфраструктуре оператора инвестиционной платформы	Получение уведомления от инвестора или самостоятельное выявление оператором инвестиционной платформы факта заключения договора инвестирования без согласия инвестора в результате НСД к информационной инфраструктуре оператора инвестиционной платформы	Нет требования к бизнес-данным инцидента защиты информации
							[FM_OIP_5]	Инцидент, связанный с заключением договора инвестирования без согласия лица, привлекающего инвестиции, в результате НСД к информационной инфраструктуре оператора инвестиционной платформы	Получение уведомления от лица, привлекающего инвестиции, или самостоятельное выявление оператором инвестиционной платформы факта заключения договора инвестирования без согласия лица, привлекающего инвестиции, в результате НСД к информационной инфраструктуре оператора инвестиционной платформы	Нет требования к бизнес-данным инцидента защиты информации
						[DT_FS]	[DT_FS_OIP_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором инвестиционной платформы	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором инвестиционной платформы	-

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
							[DT_FS_OIP_2]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором инвестиционной платформы, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – оператором инвестиционной платформы, не превышающего 24 часов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором инвестиционной платформы, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – оператором инвестиционной платформы, не превышающего 24 часов	-
				[investmentBySecurities]	Технологический процесс, обеспечивающий инвестирование с использованием инвестиционной платформы путем приобретения эмиссионных ценных бумаг, размещаемых с использованием инвестиционной платформы	[FM]	[FM_OIP_3]	Инцидент, связанный с заключением договора инвестирования на основании заявки инвестора, сформированной без его согласия, в том числе на основании модифицированной заявки инвестора	Получение уведомления от инвестора или самостоятельное выявление оператором инвестиционной платформы факта заключения договора инвестирования на основании заявки инвестора, сформированной без его согласия, в том числе на основании модифицированной заявки инвестора	Нет требования к бизнес-данным инцидента защиты информации
							[FM_OIP_4]	Инцидент, связанный с заключением договора инвестирования без согласия инвестора в результате НСД к информационной инфраструктуре оператора инвестиционной платформы	Получение уведомления от инвестора или самостоятельное выявление оператором инвестиционной платформы факта заключения договора инвестирования без согласия инвестора в результате НСД к информационной инфраструктуре оператора инвестиционной платформы	Нет требования к бизнес-данным инцидента защиты информации

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
							[FM_OIP_5]	Инцидент, связанный с заключением договора инвестирования без согласия лица, привлекающего инвестиции, в результате НСД к информационной инфраструктуре оператора инвестиционной платформы	Получение уведомления от лица, привлекающего инвестиции, или самостоятельное выявление оператором инвестиционной платформы факта заключения договора инвестирования без согласия лица, привлекающего инвестиции, в результате НСД к информационной инфраструктуре оператора инвестиционной платформы	Нет требования к бизнес-данным инцидента защиты информации
						[DT_FS]	[DT_FS_OIP_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором инвестиционной платформы	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором инвестиционной платформы	-
							[DT_FS_OIP_2]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором инвестиционной платформы, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – оператором инвестиционной платформы, не превышающего 24 часов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором инвестиционной платформы, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – оператором инвестиционной платформы, не превышающего 24 часов	-

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
				[investmentByUDR]	Технологический процесс, обеспечивающий инвестирование с использованием инвестиционной платформы путем приобретения утилитарных цифровых прав	[FM]	[FM_OIP_3]	Инцидент, связанный с заключением договора инвестирования на основании заявки инвестора, сформированной без его согласия, в том числе на основании модифицированной заявки инвестора	Получение уведомления от инвестора или самостоятельное выявление оператором инвестиционной платформы факта заключения договора инвестирования на основании заявки инвестора, сформированной без его согласия, в том числе на основании модифицированной заявки инвестора	Нет требования к бизнес-данным инцидента защиты информации
							[FM_OIP_4]	Инцидент, связанный с заключением договора инвестирования без согласия инвестора в результате НСД к информационной инфраструктуре оператора инвестиционной платформы	Получение уведомления от инвестора или самостоятельное выявление оператором инвестиционной платформы факта заключения договора инвестирования без согласия инвестора в результате НСД к информационной инфраструктуре оператора инвестиционной платформы	Нет требования к бизнес-данным инцидента защиты информации
							[FM_OIP_5]	Инцидент, связанный с заключением договора инвестирования без согласия лица, привлекающего инвестиции, в результате НСД к информационной инфраструктуре оператора инвестиционной платформы	Получение уведомления от лица, привлекающего инвестиции, или самостоятельное выявление оператором инвестиционной платформы факта заключения договора инвестирования без согласия лица, привлекающего инвестиции, в результате НСД к информационной инфраструктуре оператора инвестиционной платформы	Нет требования к бизнес-данным инцидента защиты информации

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
							[FM_OIP_6]	Инцидент, связанный с возникновением, распоряжением или передачей утилитарных цифровых прав в результате НСД к информационной инфраструктуре оператора инвестиционной платформы	Выявление оператором инвестиционной платформы факта возникновения, распоряжения или передачи утилитарных цифровых прав в результате НСД к информационной инфраструктуре оператора инвестиционной платформы	Нет требования к бизнес-данным инцидента защиты информации
						[DT_FS]	[DT_FS_OIP_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором инвестиционной платформы	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором инвестиционной платформы	-
							[DT_FS_OIP_2]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором инвестиционной платформы, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – оператором инвестиционной платформы, не превышающего 24 часов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором инвестиционной платформы, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – оператором инвестиционной платформы, не превышающего 24 часов	-
				[investmentByDFA]	Технологический процесс, обеспечивающий инвестирование с использованием инвестиционной платформы путем приобретения цифровых финансовых активов	[FM]	[FM_OIP_3]	Инцидент, связанный с заключением договора инвестирования на основании заявки инвестора, сформированной без его согласия, в том числе на основании модифицированной заявки инвестора	Получение уведомления от инвестора или самостоятельное выявление оператором инвестиционной платформы факта заключения договора инвестирования на основании заявки инвестора, сформированной без его согласия, в том числе на основании модифицированной заявки инвестора	Нет требования к бизнес-данным инцидента защиты информации

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
							[FM_OIP_4]	Инцидент, связанный с заключением договора инвестирования без согласия инвестора в результате НСД к информационной инфраструктуре оператора инвестиционной платформы	Получение уведомления от инвестора или самостоятельное выявление оператором инвестиционной платформы факта заключения договора инвестирования без согласия инвестора в результате НСД к информационной инфраструктуре оператора инвестиционной платформы	Нет требования к бизнес-данным инцидента защиты информации
							[FM_OIP_5]	Инцидент, связанный с заключением договора инвестирования без согласия лица, привлекающего инвестиции, в результате НСД к информационной инфраструктуре оператора инвестиционной платформы	Получение уведомления от лица, привлекающего инвестиции, или самостоятельное выявление оператором инвестиционной платформы факта заключения договора инвестирования без согласия лица, привлекающего инвестиции, в результате НСД к информационной инфраструктуре оператора инвестиционной платформы	Нет требования к бизнес-данным инцидента защиты информации
							[FM_OIP_7]	Инцидент, связанный с возникновением, распоряжением или передачей цифровых финансовых активов в результате НСД к информационной инфраструктуре оператора инвестиционной платформы	Выявление оператором инвестиционной платформы факта возникновения, распоряжения или передачи цифровых финансовых активов в результате НСД к информационной инфраструктуре оператора инвестиционной платформы	Нет требования к бизнес-данным инцидента защиты информации
						[DT_FS]	[DT_FS_OIP_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором инвестиционной платформы	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором инвестиционной платформы	-

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
							[DT_FS_OIP_2]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором инвестиционной платформы, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – оператором инвестиционной платформы, не превышающего 24 часов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором инвестиционной платформы, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – оператором инвестиционной платформы, не превышающего 24 часов	-
[OFP]	Осуществление деятельности оператора финансовой платформы			[enableMakeTransaction]	Технологический процесс, обеспечивающий возможность совершения участниками финансовой платформы финансовых сделок с использованием финансовой платформы	[FM]	[FM_OFP_1]	Инцидент, связанный с переводом активов потребителя финансовых услуг со специального счета на основании требования потребителя финансовых услуг, сформированного без его согласия, в том числе на основании модифицированного требования потребителя финансовых услуг	Получение уведомления от потребителя финансовых услуг или самостоятельное выявление оператором финансовой платформы факта перевода активов потребителя финансовых услуг со специального счета на основании требования потребителя финансовых услуг, сформированного без его согласия, в том числе на основании модифицированного требования потребителя финансовых услуг	Нет требования к бизнес-данным инцидента защиты информации
							[FM_OFP_2]	Инцидент, связанный с переводом активов потребителя финансовых услуг со специального счета в результате НСД к информационной инфраструктуре оператора финансовой платформы	Получение уведомления от потребителя финансовых услуг или самостоятельное выявление оператором финансовой платформы факта перевода активов потребителя финансовых услуг со специального счета в результате НСД к информационной инфраструктуре оператора финансовой платформы	Нет требования к бизнес-данным инцидента защиты информации

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
							[FM_OFP_3]	Инцидент, связанный с совершением финансовых сделок на основании заявки потребителя финансовых услуг, сформированной без его согласия, в том числе на основании модифицированной заявки потребителя финансовых услуг	Получение уведомления от потребителя финансовых услуг или самостоятельное выявление оператором финансовой платформы факта совершения финансовых сделок на основании заявки потребителя финансовых услуг, сформированной без его согласия, в том числе на основании модифицированной заявки потребителя финансовых услуг	Нет требования к бизнес-данным инцидента защиты информации
							[FM_OFP_4]	Инцидент, связанный с совершением финансовых сделок в результате НСД к информационной инфраструктуре оператора финансовой платформы или инфраструктуры взаимодействия потребителя финансовых услуг и финансовой платформы	Получение уведомления от потребителя финансовых услуг или самостоятельное выявление оператором финансовой платформы факта совершения финансовых сделок в результате НСД к информационной инфраструктуре оператора финансовой платформы или инфраструктуры взаимодействия потребителя финансовых услуг и финансовой платформы	Нет требования к бизнес-данным инцидента защиты информации
						[DT_FS]	[DT_FS_OFP_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором финансовой платформы	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором финансовой платформы	-

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
							[DT_FS_OFP_2]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором финансовой платформы, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – оператором финансовой платформы, не превышающего 2 часов для организаций, обязанных соблюдать стандартный уровень защиты информации, на период более 4 часов для иных организаций	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором финансовой платформы, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – оператором финансовой платформы, не превышающего 2 часов для организаций, обязанных соблюдать стандартный уровень защиты информации, на период более 4 часов для иных организаций	-
[OIDFA]	Операторы информационных систем, в которых осуществляется выпуск цифровых финансовых активов (ЦФА)			[accessToPlatform]	Технологический процесс, обеспечивающий доступ к информационной системе, в том числе ведение реестра пользователей информационной системы	[DT_FS]	[DT_FS_OIDFA_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором информационной системы, в которой осуществляется выпуск цифровых финансовых активов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором информационной системы, в которой осуществляется выпуск цифровых финансовых активов	-

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
							[DT_FS_OIDFA_2]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором информационной системы, в которой осуществляется выпуск цифровых финансовых активов, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – оператором информационной системы, в которой осуществляется выпуск цифровых финансовых активов, не превышающего 6 часов для организаций, обязанных соблюдать стандартный уровень защиты информации, 12 часов для иных организаций	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором информационной системы, в которой осуществляется выпуск цифровых финансовых активов, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – оператором информационной системы, в которой осуществляется выпуск цифровых финансовых активов, не превышающего 6 часов для организаций, обязанных соблюдать стандартный уровень защиты информации, 12 часов для иных организаций	-
				[issueDFA]	Технологический процесс, обеспечивающий выпуск цифровых финансовых активов в информационной системе	[FM]	[FM_OIDFA_1]	Инцидент, связанный с выпуском ЦФА на основании запроса о выпуске ЦФА, сформированного без согласия лица, выпускающего ЦФА, в том числе на основании модифицированного запроса	Получение уведомления от лица, выпускающего ЦФА, или самостоятельное выявление оператором информационной системы, в которой осуществляется выпуск цифровых финансовых активов, факта выпуска ЦФА на основании запроса о выпуске ЦФА, сформированного без согласия лица, выпускающего ЦФА, в том числе на основании модифицированного запроса	Нет требования к бизнес-данным инцидента защиты информации

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
							[FM_OIDFA_2]	Инцидент, связанный с выпуском ЦФА в результате НСД к инфраструктуре оператора информационной системы, в которой осуществляется выпуск цифровых финансовых активов	Выявление оператором информационной системы, в которой осуществляется выпуск цифровых финансовых активов, факта выпуска ЦФА в результате НСД к инфраструктуре оператора информационной системы	Нет требования к бизнес-данным инцидента защиты информации
							[FM_OIDFA_3]	Инцидент, связанный с выпуском ЦФА в результате эксплуатации недостатков (уязвимостей) алгоритма (алгоритмов), обеспечивающего тождественность информации, содержащейся во всех базах данных, составляющих распределенный реестр (алгоритмы консенсуса)	Выявление оператором информационной системы, в которой осуществляется выпуск цифровых финансовых активов факта выпуска ЦФА в результате эксплуатации недостатков (уязвимостей) алгоритма (-ов), обеспечивающего (-их) тождественность информации, содержащейся во всех базах данных, составляющих распределенный реестр (алгоритмы консенсуса)	Нет требования к бизнес-данным инцидента защиты информации
						[DT_FS]	[DT_FS_OIDFA_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором информационной системы, в которой осуществляется выпуск цифровых финансовых активов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором информационной системы, в которой осуществляется выпуск цифровых финансовых активов	-

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
							[DT_FS_OIDFA_3]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором информационной системы, в которой осуществляется выпуск цифровых финансовых активов, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – оператором информационной системы, в которой осуществляется выпуск цифровых финансовых активов, не превышающего 24 часов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором информационной системы, в которой осуществляется выпуск цифровых финансовых активов, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – оператором информационной системы, в которой осуществляется выпуск цифровых финансовых активов, не превышающего 24 часов	-
				[circulationDFA]	Технологический процесс, обеспечивающий обращение цифровых финансовых активов в информационной системе, в том числе погашение записей о цифровых финансовых активах	[FM]	[FM_OIDFA_4]	Инцидент, связанный с обращением ЦФА на основании запроса об обращении ЦФА, сформированного без согласия владельца ЦФА, в том числе на основании модифицированного запроса	Получение уведомления от владельца ЦФА или самостоятельное выявление оператором информационной системы, в которой осуществляется выпуск цифровых финансовых активов, факта обращения ЦФА на основании запроса об обращении ЦФА, сформированного без согласия владельца ЦФА, в том числе на основании модифицированного запроса	Нет требования к бизнес-данным инцидента защиты информации
							[FM_OIDFA_5]	Инцидент, связанный с обращением ЦФА в результате НСД к инфраструктуре оператора информационной системы, в которой осуществляется выпуск цифровых финансовых активов	Выявление оператором информационной системы, в которой осуществляется выпуск цифровых финансовых активов, факта обращения ЦФА в результате НСД к инфраструктуре оператора информационной системы	Нет требования к бизнес-данным инцидента защиты информации

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
							[FM_OIDFA_6]	Инцидент, связанный с обращением ЦФА в результате эксплуатации недостатков (уязвимостей) алгоритма (-ов), обеспечивающего (-их) тождественность информации, содержащейся во всех базах данных, составляющих распределенный реестр (алгоритмы консенсуса)	Выявление оператором информационной системы, в которой осуществляется выпуск цифровых финансовых активов факта обращения ЦФА в результате эксплуатации недостатков (уязвимостей) алгоритма (-ов), обеспечивающего (-их) тождественность информации, содержащейся во всех базах данных, составляющих распределенный реестр (алгоритмы консенсуса)	Нет требования к бизнес-данным инцидента защиты информации
						[DT_FS]	[DT_FS_OIDFA_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором информационной системы, в которой осуществляется выпуск цифровых финансовых активов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором информационной системы, в которой осуществляется выпуск цифровых финансовых активов	-

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
							[DT_FS_OIDFA_2]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором информационной системы, в которой осуществляется выпуск цифровых финансовых активов, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – оператором информационной системы, в которой осуществляется выпуск цифровых финансовых активов, не превышающего 6 часов для организаций, обязанных соблюдать стандартный уровень защиты информации, 12 часов для иных организаций	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором информационной системы, в которой осуществляется выпуск цифровых финансовых активов, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – оператором информационной системы, в которой осуществляется выпуск цифровых финансовых активов, не превышающего 6 часов для организаций, обязанных соблюдать стандартный уровень защиты информации, 12 часов для иных организаций	-
				[accountingDFA]	Технологический процесс, обеспечивающий внесение записей оператором информационной системы в соответствии с частью 2 статьи 6 Федерального закона от 31 июля 2020 года N° 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации»	[FM]	[FM_OIDFA_7]	Инцидент, связанный с внесением записей в реестр оператора информационных систем, в которых осуществляется выпуск цифровых финансовых активов, в результате НСД к инфраструктуре оператора	Выявление оператором информационных систем, в которых осуществляется выпуск цифровых финансовых активов, факта внесения записей в реестр оператора информационных систем, в которых осуществляется выпуск цифровых финансовых активов, в результате НСД к инфраструктуре оператора	Нет требования к бизнес-данным инцидента защиты информации

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
						[DT_FS]	[DT_FS_OIDFA_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором информационной системы, в которой осуществляется выпуск цифровых финансовых активов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором информационной системы, в которой осуществляется выпуск цифровых финансовых активов	-
							[DT_FS_OIDFA_4]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором информационной системы, в которой осуществляется выпуск цифровых финансовых активов, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – оператором информационной системы, в которой осуществляется выпуск цифровых финансовых активов, не превышающего 2 часов для организаций, обязанных соблюдать стандартный уровень защиты информации, 4 часов для иных организаций	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором информационной системы, в которой осуществляется выпуск цифровых финансовых активов, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – оператором информационной системы, в которой осуществляется выпуск цифровых финансовых активов, не превышающего 2 часов для организаций, обязанных соблюдать стандартный уровень защиты информации, 4 часов для иных организаций	-

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
				[accounting-OfHoldersDFA]	Технологический процесс, обеспечивающий внесение учетных записей в реестр владельцев акций непубличных акционерных обществ, осуществляющих выпуск цифровых финансовых активов, удостоверяющих права участия в капитале указанных непубличных акционерных обществ	[FM]	[FM_OIDFA_8]	Инцидент, связанный с внесением учетных записей в реестр владельцев акций непубличных акционерных обществ, выпущенных в виде цифровых финансовых активов, в результате НСД к инфраструктуре оператора информационных систем, в которых осуществляется выпуск цифровых финансовых активов	Выявление оператором информационных систем, в которых осуществляется выпуск цифровых финансовых активов, факта внесения учетных записей в реестр владельцев акций непубличных акционерных обществ, выпущенных в виде цифровых финансовых активов, в результате НСД к инфраструктуре оператора информационных систем, в которых осуществляется выпуск цифровых финансовых активов	Нет требования к бизнес-данным инцидента защиты информации
						[DT_FS]	[DT_FS_OIDFA_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором информационной системы, в которой осуществляется выпуск цифровых финансовых активов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором информационной системы, в которой осуществляется выпуск цифровых финансовых активов	-

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
							[DT_FS_OIDFA_3]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – оператора информационной системы, в которой осуществляется выпуск цифровых финансовых активов, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – оператора информационной системы, в которой осуществляется выпуск цифровых финансовых активов, не превышающего 24 часов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – оператора информационной системы, в которой осуществляется выпуск цифровых финансовых активов, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – оператора информационной системы, в которой осуществляется выпуск цифровых финансовых активов, не превышающего 24 часов	-
				[interactionWithOEDFA]	Технологический процесс, обеспечивающий взаимодействие с оператором обмена цифровых финансовых активов	[DT_FS]	[DT_FS_OIDFA_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором информационной системы, в которой осуществляется выпуск цифровых финансовых активов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором информационной системы, в которой осуществляется выпуск цифровых финансовых активов	-

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
							[DT_FS_OIDFA_2]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором информационной системы, в которой осуществляется выпуск цифровых финансовых активов, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – оператором информационной системы, в которой осуществляется выпуск цифровых финансовых активов, не превышающего 6 часов для организаций, обязанных соблюдать стандартный уровень защиты информации, 12 часов для иных организаций	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором информационной системы, в которой осуществляется выпуск цифровых финансовых активов, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – оператором информационной системы, в которой осуществляется выпуск цифровых финансовых активов, не превышающего 6 часов для организаций, обязанных соблюдать стандартный уровень защиты информации, 12 часов для иных организаций	-
				[monitoring-OfImmutability]	Технологический процесс, обеспечивающий мониторинг тождественности информации, содержащейся во всех базах данных, составляющих распределенный реестр	[DT_FS]	[DT_FS_OIDFA_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором информационной системы, в которой осуществляется выпуск цифровых финансовых активов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором информационной системы, в которой осуществляется выпуск цифровых финансовых активов	-

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
							[DT_FS_OIDFA_2]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором информационной системы, в которой осуществляется выпуск цифровых финансовых активов, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – оператором информационной системы, в которой осуществляется выпуск цифровых финансовых активов, не превышающего 6 часов для организаций, обязанных соблюдать стандартный уровень защиты информации, 12 часов для иных организаций	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором информационной системы, в которой осуществляется выпуск цифровых финансовых активов, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – оператором информационной системы, в которой осуществляется выпуск цифровых финансовых активов, не превышающего 6 часов для организаций, обязанных соблюдать стандартный уровень защиты информации, 12 часов для иных организаций	-
[OEDFA]	Операторы обмена цифровых финансовых активов (ЦФА)			[enableDeals-WithDFA]	Технологический процесс, обеспечивающий возможность совершения сделок с цифровыми финансовыми активами	[FM]	[FM_OEDFA_1]	Инцидент, связанный с совершением сделок с цифровыми финансовыми активами на основании запроса на обмен ЦФА, сформированного без согласия лица, обменивающего ЦФА, в том числе на основании модифицированного запроса	Получение уведомления от лица, обменивающего ЦФА, или самостоятельное выявление оператором обмена цифровых финансовых активов факта совершения сделки с цифровыми финансовыми активами на основании запроса на обмен ЦФА, сформированного без согласия лица, обменивающего ЦФА, в том числе на основании модифицированного запроса	Нет требования к бизнес-данным инцидента защиты информации

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
							[FM_OEDFA_2]	Инцидент, связанный с совершением сделок с цифровыми финансовыми активами в результате НСД к инфраструктуре оператора обмена цифровых финансовых активов или инфраструктуры взаимодействия лица, обменивающего ЦФА, и информационной системы, в которой осуществляется обмен цифровых финансовых активов	Получение уведомления от лица, обменивающего ЦФА, или самостоятельное выявление оператором обмена цифровых финансовых активов факта совершения сделки с цифровыми финансовыми активами в результате НСД к инфраструктуре оператора обмена цифровых финансовых активов или инфраструктуры взаимодействия лица, обменивающего ЦФА, и информационной системы, в которой осуществляется обмен цифровых финансовых активов	Нет требования к бизнес-данным инцидента защиты информации
							[FM_OEDFA_3]	Инцидент, связанный с совершением сделок с цифровыми финансовыми активами в результате эксплуатации недостатков (уязвимостей) алгоритма (-ов), обеспечивающего (-их) тождественность информации, содержащейся во всех базах данных, составляющих распределенный реестр	Самостоятельное выявление оператором обмена цифровых финансовых активов факта совершения сделки с цифровыми финансовыми активами в результате эксплуатации недостатков (уязвимостей) алгоритма (-ов), обеспечивающего (-их) тождественность информации, содержащейся во всех базах данных, составляющих распределенный реестр (алгоритмы консенсуса)	Нет требования к бизнес-данным инцидента защиты информации
							[FM_OEDFA_4]	Инцидент, связанный с передачей цифровых финансовых активов на цифровой кошелек отличный от цифрового кошелька получателя ЦФА в результате НСД к инфраструктуре оператора обмена цифровых финансовых активов	Получение уведомления от получателя ЦФА или самостоятельное выявление оператором обмена цифровых финансовых активов факта передачи ЦФА на цифровой кошелек, отличный от цифрового кошелька получателя ЦФА	Нет требования к бизнес-данным инцидента защиты информации

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
						[DT_FS]	[DT_FS_OEDFA_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором обмена цифровых финансовых активов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором обмена цифровых финансовых активов	-
							[DT_FS_OEDFA_2]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором обмена цифровых финансовых активов, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – оператором обмена цифровых финансовых активов, не превышающего 6 часов для организаций, обязанных соблюдать стандартный уровень защиты информации, 12 часов для иных организаций	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором обмена цифровых финансовых активов, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – оператором обмена цифровых финансовых активов, не превышающего 6 часов для организаций, обязанных соблюдать стандартный уровень защиты информации, 12 часов для иных организаций	-
				[interactionWithOIDFA]	Технологический процесс, обеспечивающий взаимодействие с оператором информационной системы	[DT_FS]	[DT_FS_OEDFA_1]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором обмена цифровых финансовых активов	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором обмена цифровых финансовых активов	-

Код вида (направления) деятельности финансовой организации первого уровня	Наименование вида (направления) деятельности финансовой организации первого уровня	Код вида (направления) деятельности финансовой организации второго уровня	Наименование вида (направления) деятельности финансовой организации второго уровня	Код технологического процесса	Наименование технологического процесса	Код типа инцидента	Код инцидента	Наименование инцидента	Критерий информирования	Бизнес-данные инцидента защиты информации
							[DT_FS_OEDFA_2]	Инцидент, связанный с превышением допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором обмена цифровых финансовых активов, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – оператором обмена цифровых финансовых активов, не превышающего 6 часов для организаций, обязанных соблюдать стандартный уровень защиты информации, 12 часов для иных организаций	Выявление факта превышения допустимой доли деградации технологического процесса, установленной финансовой организацией – оператором обмена цифровых финансовых активов, а также допустимого времени простоя и (или) деградации технологического процесса, установленного финансовой организацией – оператором обмена цифровых финансовых активов, не превышающего 6 часов для организаций, обязанных соблюдать стандартный уровень защиты информации, 12 часов для иных организаций	-

ПРИЛОЖЕНИЕ 12. ФОРМА ПРЕДСТАВЛЕНИЯ ДАННЫХ NTF_ISI_DETECT – ФОРМА ПРЕДСТАВЛЕНИЯ УЧАСТНИКАМИ ИНФОРМАЦИОННОГО ОБМЕНА ДАННЫХ О ВЫЯВЛЕНИИ ИНЦИДЕНТА ЗАЩИТЫ ИНФОРМАЦИИ

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип уведомления	Тип уведомления	O	-	[NTF_ISI_Detect]	Предзаполненное поле
2	Дата и время	Дата и время выявления инцидента защиты информации	O	-	В соответствии с RFC 3339	По московскому времени [UTC +03:00]
3	Классификация инцидента защиты информации	Код вида (направления) деятельности финансовой организации	O	-	Выбор одного значения из списка: Из классификатора «Классификатор инцидентов защиты информации и инцидентов операционной надежности, в разрезе видов деятельности кредитных организаций, некредитных финансовых организаций и субъектов национальной платежной системы и составляющих их технологических процессов», приведенного в приложении 11	При наличии кода вида (направления) деятельности финансовой организации первого и второго уровня они заполняются через «.», например: [Код 1].[Код 2]
4		Код технологического процесса	O	-	Выбор одного значения из списка: Из классификатора «Классификатор инцидентов защиты информации и инцидентов операционной надежности, в разрезе видов деятельности кредитных организаций, некредитных финансовых организаций и субъектов национальной платежной системы и составляющих их технологических процессов», приведенного в приложении 11 Перечень зависит от поля «Код вида (направления) деятельности финансовой организации»	-
5		Код источника риска	O	-	Выбор одного значения из списка: Из классификатора «Источники риска», приведенного в приложении 28	-

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
6		Код типа инцидента	О	-	Выбор одного значения из списка: Из классификатора «Классификатор инцидентов защиты информации и инцидентов операционной надежности, в разрезе видов деятельности кредитных организаций, некредитных финансовых организаций и субъектов национальной платежной системы и составляющих их технологических процессов», приведенного в приложении 11 Перечень зависит от поля «Код технологического процесса»	-
7		Код инцидента	О	-	Выбор одного значения из списка: Из классификатора «Классификатор инцидентов защиты информации и инцидентов операционной надежности, в разрезе видов деятельности кредитных организаций, некредитных финансовых организаций и субъектов национальной платежной системы и составляющих их технологических процессов», приведенного в приложении 11 Перечень зависит от поля «Код типа инцидента защиты информации»	-
8	Бизнес-данные финансового инцидента	Набор данных в зависимости от инцидента	УО	«Код типа финансового инцидента» = [FM] и предусмотрено заполнение бизнес-данных	Из классификатора «Классификатор инцидентов защиты информации и инцидентов операционной надежности, в разрезе видов деятельности кредитных организаций, некредитных финансовых организаций и субъектов национальной платежной системы и составляющих их технологических процессов», приведенного в приложении 11	Состав данных зависит от «Код инцидента защиты информации»

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
9		Вид актива			Текстовое поле	-
10		Количество активов			Целое число >0	-
11		Стоимость единичного актива			Сумма в рублях с точностью до двух знаков после запятой	-
12		Цифровой отпечаток устройства			Цифровой отпечаток устройства, собранный в соответствии с рекомендациями Банка России	Заполняется при наличии технической возможности получить цифровой отпечаток устройства, с которого осуществлялась финансовая операция
13	Связь с другими уведомлениями	Вид связанного уведомления	УО	Заполняется в случае направления ранее в Банк России уведомления, связанного с текущим	Выбор одного значения из списка: [NTF_OWC] [NTF_ISI] [NTF_ORI] [NTF_CI] [NTF_CA] [NTF_VLN]	[NTF_OWC] – уведомление о выявленных случаях и (или) попытках осуществления переводов денежных средств без согласия клиента, а также о выявленных случаях и (или) попытках осуществления операций, направленных на совершение финансовых сделок с использованием финансовой платформы без волеизъявления участника финансовой платформы [NTF_ISI] – уведомление о выявлении инцидента защиты информации или результатах расследования инцидента защиты информации [NTF_ORI] – уведомление о выявлении инцидента операционной надежности или о результатах расследования инцидента операционной надежности [NTF_CI] – уведомление о компьютерных инцидентах [NTF_CA] – уведомления о компьютерных атаках [NTF_VLN] – уведомление о выявленных уязвимостях
14		Тип связи с другими уведомлениями			Выбор одного значения из списка: [Предшествующее событие] [Дочернее событие] [Связанное событие] [Уточнение сведений о событии]	-

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
15		Регистрационный номер уведомления			В соответствии с форматом АСОИ ФинЦЕРТ	Идентификатор уведомления или ответа на запрос, ранее направленного в ФинЦЕРТ участником информационного обмена
16	Ограничительный маркер TLP	Ограничительный маркер на распространение сведений из данного уведомления	Н	-	Выбор одного значения из списка: [TLP: WHITE] [TLP: GREEN] [TLP: AMBER] [TLP: RED]	В соответствии с обозначениями, принятыми в протоколе TLP По умолчанию [TLP: GREEN], если не указано иное
17	Необходимость привлечения ФинЦЕРТ	Необходимость привлечения ФинЦЕРТ	УО	При необходимости	[Да]	Необходимость привлечения ФинЦЕРТ для проведения расследования инцидента защиты информации, результаты которого должны быть направлены уведомлением о расследовании

ПРИЛОЖЕНИЕ 13. ФОРМА ПРЕДСТАВЛЕНИЯ ДАННЫХ NTF_ISI_DATALEAK – ФОРМА ПРЕДСТАВЛЕНИЯ УЧАСТНИКАМИ ИНФОРМАЦИОННОГО ОБМЕНА ДАННЫХ О ВЫЯВЛЕНИИ НЕЗАКОННОГО РАСКРЫТИЯ БАНКОВСКОЙ ТАЙНЫ И (ИЛИ) ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ В СООТВЕТСТВИИ С НОРМАТИВНЫМИ АКТАМИ БАНКА РОССИИ

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип уведомления	Тип уведомления	О	-	[NTF_ISI_DataLeak]	Предзаполненное поле
2	Дата и время	Дата выявления факта незаконного раскрытия банковской тайны, персональных данных и (или) иных данных клиентов или сотрудников участника информационного обмена	О	-	В соответствии с RFC 3339	По московскому времени [UTC +03:00]
3	Общие сведения о факте незаконного раскрытия информации	Тип незаконно раскрытой информации	О	-	[Банковская тайна] [Персональные данные] [Иная защищаемая информация]	-
4		Предполагаемые причины незаконного раскрытия информации	О	-	Текстовое поле	Описание событий, которые привели к незаконному раскрытию информации
5		Предполагаемый вред, нанесенный правам субъектов	О	-	Текстовое поле	Описание потенциального вреда, который может быть нанесен субъектам при использовании незаконно раскрытой информации
6	Характеристики незаконно раскрытой информации	Тип субъекта, чья информация была раскрыта	О	-	[Employee] [Client] [Partner] [Other]	[Employee] – Работники финансовой организации [Client] – Клиенты финансовой организации [Partner] – Партнеры, контрагенты, подрядчики и т. д. финансовой организации [Other] – Другое
7		Состав незаконно раскрытой информации	О	-	Текстовое поле	Описание состава данных незаконно раскрытой информации
8		Количество записей незаконно раскрытой информации	УО	В случае если количество незаконно раскрытой информации можно измерить количеством записей (например, строк БД)	Число	Фактическое или предполагаемое количество записей
9		Актуальность незаконно раскрытой информации	О	-	[Данные актуальны] [Данные неактуальны]	-
10	Сведения о лице, уполномоченном оператором на взаимодействие с Роскомнадзором по инциденту	ФИО лица, уполномоченного оператором на взаимодействие с Роскомнадзором по инциденту	УО	«Тип незаконно раскрытой информации» = [Персональные данные]	Текстовое поле	-

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
11		Мобильный телефон лица, уполномоченного на взаимодействие с Роскомнадзором по инциденту			В соответствии с российской системой и планом нумерации	-
12		Адрес электронной почты для отправки информации об уведомлении			В формате e-mail-адреса	-
13	Связь с другими уведомлениями	Вид связанного уведомления	УО	Заполняется в случае направления ранее в Банк России уведомления, связанного с текущим	[NTF_OWC] [NTF_ISI] [NTF_ORI] [NTF_CI] [NTF_CA] [NTF_VLN]	[NTF_OWC] – уведомление о выявленных случаях и (или) попытках осуществления переводов денежных средств без согласия клиента, а также о выявленных случаях и (или) попытках осуществления операций, направленных на совершение финансовых сделок с использованием финансовой платформы без волеизъявления участника финансовой платформы [NTF_ISI] – уведомление о выявлении инцидента защиты информации или результатах расследования инцидента защиты информации [NTF_ORI] – уведомление о выявлении инцидента операционной надежности или о результатах расследования инцидента операционной надежности [NTF_CI] – уведомление о компьютерных инцидентах [NTF_CA] – уведомления о компьютерных атаках [NTF_VLN] – уведомление о выявленных уязвимостях
14		Тип связи с другими уведомлениями			[Предшествующее событие] [Дочернее событие] [Связанное событие] [Уточнение сведений о событии]	-
15		Регистрационный номер уведомления			В соответствии с форматом АСОИ ФинЦЕРТ	Идентификатор уведомления или ответа на запрос, ранее направленного в ФинЦЕРТ участником информационного обмена

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
16	Ограничительный маркер TLP	Ограничительный маркер на распространение сведений из данного уведомления	Н	-	Выбор одного значения из списка: [TLP: WHITE] [TLP: GREEN] [TLP: AMBER] [TLP: RED]	В соответствии с обозначениями, принятыми в протоколе TLP. По умолчанию [TLP: GREEN], если не указано иное
17	Необходимость привлечения ФинЦЕРТ	Необходимость привлечения ФинЦЕРТ	УО	При необходимости	[Да]	Необходимость привлечения ФинЦЕРТ для проведения расследования незаконного раскрытия информации, результаты которого должны быть направлены уведомлением о расследовании

ПРИЛОЖЕНИЕ 14. ФОРМА ПРЕДСТАВЛЕНИЯ ДАННЫХ NTF_ISI_INVESTIGATION – ФОРМА ПРЕДСТАВЛЕНИЯ УЧАСТНИКАМИ ИНФОРМАЦИОННОГО ОБМЕНА ДАННЫХ О РЕЗУЛЬТАТАХ РАССЛЕДОВАНИЯ ИНЦИДЕНТА ЗАЩИТЫ ИНФОРМАЦИИ ИЛИ НЕЗАКОННОГО РАСКРЫТИЯ БАНКОВСКОЙ ТАЙНЫ И (ИЛИ) ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ В СООТВЕТСТВИИ С НОРМАТИВНЫМИ АКТАМИ БАНКА РОССИИ

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип уведомления	Тип уведомления	O	-	[NTF_ISI_Investigation]	Предзаполненное поле
2	Связь с уведомлением о выявлении инцидента защиты информации или или незаконного раскрытия банковской тайны, персональных данных и (или) иных данных клиентов или сотрудников участника информационного обмена	Идентификатор (-ы) уведомления о выявлении инцидента защиты информации или незаконного раскрытия банковской тайны, персональных данных и (или) иных данных клиентов или сотрудников участника информационного обмена	O	-	В соответствии с форматом АСОИ ФинЦЕРТ. При указании нескольких идентификаторов, необходимо их перечислять через «;»	Идентификатор (-ы) уведомления или ответа на запрос, ранее направленного в ФинЦЕРТ участником информационного обмена. В случае если уведомление о результатах расследования описывает сценарий атаки, который привел к нескольким инцидентам защиты информации или событиям незаконного раскрытия банковской тайны, персональных данных и (или) иных данных клиентов или сотрудников участника информационного обмена, указываются все связанные уведомления о выявлении инцидента защиты информации или незаконного раскрытия банковской тайны, персональных данных и (или) иных данных клиентов или сотрудников участника информационного обмена
3	Дата и время	Дата и время фактического свершения инцидента защиты информации	O	-	В соответствии с RFC 3339	По московскому времени [UTC +03:00]

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
4	Уточнение данных, содержащихся в уведомлении о выявлении инцидента защиты информации	Код вида (направления) деятельности финансовой организации	УО	При необходимости уточнить классификацию инцидента защиты информации, ранее предоставленную в уведомление о выявлении инцидента защиты информации	Выбор одного значения из списка: Из классификатора «Классификатор инцидентов защиты информации и инцидентов операционной надежности, в разрезе видов деятельности кредитных организаций, некредитных финансовых организаций и субъектов национальной платежной системы и составляющих их технологических процессов», приведенного в приложении 11	При наличии кода вида (направления) деятельности финансовой организации первого и второго уровня они заполняются через «.», например: [Код 1].[Код 2]
5		Код технологического процесса			Выбор одного значения из списка: Из классификатора «Классификатор инцидентов защиты информации и инцидентов операционной надежности, в разрезе видов деятельности кредитных организаций, некредитных финансовых организаций и субъектов национальной платежной системы и составляющих их технологических процессов», приведенного в приложении 11 Перечень зависит от поля «Код вида (направления) деятельности финансовой организации»	-
6		Код источника риска			Выбор одного значения из списка: Из классификатора «Источники риска», приведенного в приложении 28	-

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
7		Код типа инцидента			Выбор одного значения из списка: Из классификатора «Классификатор инцидентов защиты информации и инцидентов операционной надежности, в разрезе видов деятельности кредитных организаций, некредитных финансовых организаций и субъектов национальной платежной системы и составляющих их технологических процессов», приведенного в приложении 11 Перечень зависит от поля «Код технологического процесса»	-
8		Код инцидента			Выбор одного значения из списка: Из классификатора «Классификатор инцидентов защиты информации и инцидентов операционной надежности, в разрезе видов деятельности кредитных организаций, некредитных финансовых организаций и субъектов национальной платежной системы и составляющих их технологических процессов», приведенного в приложении 11 Перечень зависит от поля «Код типа инцидента защиты информации»	-
9	Сценарий атаки	Сценарий атаки	УО	Обязательно заполняется хотя бы одно из полей	В формате: {ID тактики 1}. {ID техники 1}: {ID тактики 2}. {ID техники 2} + {ID техники 3}: {ID тактики 3}. {ID техники 4}	Последовательный перечень идентификаторов техник и тактик проведения атаки на основании матрицы MITRE ATT&CK
10		Описание сценария атаки			Текстовое поле	Текстовое описание сценария атаки. Заполняется в случае отсутствия в матрице MITRE ATT&CK необходимых техник/тактик

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
11	Шаблон атаки (заполняется отдельно для каждой тактики «Сценария атаки»)	Идентификатор тактики	О	-	В формате: {ID тактики}. {ID техники} или текстовое поле	Идентификатор тактики, являющийся составной частью «Сценария атаки», или шаг атаки из «Описание сценария атаки»
12		Процедура	О	-	Текстовое поле	Описание процедуры, описывающей реализацию тактики
13		Наименование технологического участка, на котором реализована тактика	О	-	Выбор одного значения из списка: Из классификатора «Технологические участки», приведенного в приложении 28	-
14		Код уровня объекта/субъекта, на который была направлена атака	О	-	Выбор одного значения из списка: Из классификатора «Типы объектов и субъектов», приведенного в приложении 28	Блок заполняется отдельно для каждого объекта/субъекта, на который была направлена атака
15		Код типа объекта/субъекта, на который была направлена атака	О	-	«Выбор одного значения из списка: Из классификатора «Типы объектов и субъектов», приведенного в приложении 28 Перечень зависит от поля «Код уровня объекта/субъекта»	
16		Описание объекта информационной инфраструктуры, на который была направлена атака, в формате CPE	УО	«Код уровня объекта/субъекта» ≠ [Subject]	В формате, соответствующем рекомендациям Банка России, опубликованным на официальном сайте	
17		Идентификатор атаки	УО	Процедура соответствует атаке классификатора CAPEC	Из классификатора CAPEC	Идентификатор атаки CAPEC, соответствующий процедуре
18		Перечень используемых слабостей безопасности в процессе атаки	УО	В процессе расследования было выявлено использование слабостей безопасности	Текстовое поле При использовании нескольких слабостей безопасности перечисляются через «+»	Перечень используемых слабостей безопасности программного или аппаратного обеспечения в выбранной системе описания слабостей безопасности
19		Наименование системы описания слабостей безопасности			Выбор одного значения из списка: [CWE] [БДУ ФСТЭК]	

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
20		Перечень эксплуатируемых уязвимостей безопасности в процессе атаки	УО	В процессе расследования была выявлена эксплуатация уязвимостей безопасности	Текстовое поле При использовании нескольких уязвимостей безопасности перечисляются через «+»	Перечень эксплуатируемых уязвимостей безопасности программного или аппаратного обеспечения в выбранной системе описания уязвимостей безопасности
21		Наименование системы описания уязвимостей безопасности			Выбор одного значения из списка: [CVE] [БДУ ФСТЭК]	
22		Программное обеспечение, используемое атакующим	Н	-	Текстовое поле	При наличии соответствующей информации
23		Индикаторы компрометации	УО	В случае если в процессе расследования были выявлены индикаторы компрометации, ранее не направлявшиеся в ФинЦЕРТ	Текстовое поле или файл	-
24	Принятые меры	Принятые контрмеры	УО	Обязательно заполняется хотя бы одно из полей	Перечень идентификаторов контрмер	Перечень идентификаторов контрмер, направленных на нейтрализацию атаки и недопущение повторной атаки, на основании матрицы MITRE DEF3ND
25		Описание мер защиты			Текстовое поле	Текстовое описание принятых мер для нейтрализации атаки и недопущения повторной атаки
26	Ущерб от инцидента	Сумма прямых потерь	УО	Если такие потери являются последствиями реализации финансового инцидента и есть возможность их оценить	Сумма в рублях с точностью до двух знаков после запятой	К прямым потерям финансовой организации относятся потери, отраженные на счетах расходов и убытков в бухгалтерском учете и на приравненных к ним счетах по учету дебиторской задолженности
27		Сумма косвенных потерь	УО	Если такие потери являются последствиями реализации финансового инцидента и есть возможность их оценить	Сумма в рублях с точностью до двух знаков после запятой	Непрямые потери финансовой организации, не отраженные в бухгалтерском учете, но косвенно связанные с событиями риска реализации информационных угроз, включающие потери, определяемые расчетным методом в денежном выражении

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
28		Качественные потери	УО	Если на организацию распространяется требования об оценке таких потерь в соответствии с 716-П	[Очень высокие] [Высокие] [Средние] [Низкие]	Непрямые потери финансовой организации, не отраженные в бухгалтерском учете, но косвенно связанные с событиями риска реализации информационных угроз, включающие потери, определяемые с использованием экспертного мнения, в случае если потери не выражены в денежном выражении расчетным методом
29		Сумма потенциальных потерь	УО	Если такие потери являются последствиями реализации финансового инцидента и есть возможность их оценить	Сумма в рублях с точностью до двух знаков после запятой	Непрямые потери финансовой организации, не отраженные в бухгалтерском учете, но косвенно связанные с событиями риска реализации информационных угроз, включающие потери, не реализовавшиеся в виде прямых и косвенных потерь, которые могли бы возникнуть при реализации не выявленных финансовой организацией источников риска реализации информационных угроз и (или) при неблагоприятном стечении обстоятельств
30		Мероприятия, осуществленные кредитной организацией в целях получения возмещения по понесенным потерям	УО	Если такие мероприятия проводились/проводятся	Текстовое поле	-
31	Уникальный порядковый идентификационный номер события операционного риска	Уникальный порядковый идентификационный номер события операционного риска в базе событий, соответствующего данному инциденту	УО	Только для кредитных организаций	Текстовое поле	-

ПРИЛОЖЕНИЕ 15. ФОРМА ПРЕДСТАВЛЕНИЯ ДАННЫХ REQ_ISI_DATALEAK – ФОРМА ЗАПРОСА БАНКА РОССИИ В ЦЕЛЯХ ПОДТВЕРЖДЕНИЯ ФАКТА НЕЗАКОННОГО РАСКРЫТИЯ БАНКОВСКОЙ ТАЙНЫ И (ИЛИ) ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ В СООТВЕТСТВИИ С НОРМАТИВНЫМИ АКТАМИ БАНКА РОССИИ

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип запроса/ответа	Тип запроса/ответа	О	-	[REQ_ISI_DataLeak]	Предзаполненное поле
2	Общие данные запроса	Тип незаконно раскрытой информации	О	-	[Банковская тайна] [Персональные данные] [Иная защищаемая информация]	-
3		Описание незаконно раскрытой информации	О	-	Текстовое поле	-
4		Дата обнаружения	О	-	В соответствии с RFC 3339	По московскому времени [UTC +03:00]
5		Ссылка на объявление с раскрытой информации	УО	При наличии	Текстовое поле	-

Форма представления данных RESP_ISI_DataLeak – Форма представления ответа на запрос Банка России в целях подтверждения факта незаконного раскрытия банковской тайны и (или) защищаемой информации в соответствии с нормативными актами Банка России

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип запроса/ответа	Тип запроса/ответа	О	-	[RESP_ISI_DataLeak]	Предзаполненное поле
2	Статус	Статус выявления незаконного раскрытия банковской тайны, персональных данных и (или) иных данных клиентов или сотрудников участника информационного обмена	О	-	[Факт незаконного раскрытия выявлен, информация ранее направлялась в Банк России] [Факт незаконного раскрытия не выявлен] [Необходимо дополнительное время для рассмотрения]	-
3	Идентификатор связанного уведомления	Идентификатор уведомления о выявлении незаконного раскрытия банковской тайны, персональных данных и (или) иных данных клиентов или сотрудников участника информационного обмена	УО	«Статус» = [Да, информация ранее направлялась в Банк России]	В соответствии с форматом АСОИ ФинЦЕРТ	Идентификатор уведомления о выявлении незаконного раскрытия банковской тайны, персональных данных и (или) иных данных клиентов или сотрудников участника информационного обмена, ранее направленного в ФинЦЕРТ участником информационного обмена

ПРИЛОЖЕНИЕ 16. ФОРМА ПРЕДСТАВЛЕНИЯ ДАННЫХ NTF_ORI_DETECT – ФОРМА ПРЕДСТАВЛЕНИЯ УЧАСТНИКАМИ ИНФОРМАЦИОННОГО ОБМЕНА ДАННЫХ О ВЫЯВЛЕНИИ ИНЦИДЕНТА ОПЕРАЦИОННОЙ НАДЕЖНОСТИ

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип уведомления	Тип уведомления	O	-	[NTF_ORI_Detect]	Предзаполненное поле
2	Дата и время	Дата и время выявления инцидента операционной надежности	O	-	В соответствии с RFC 3339	По московскому времени [UTC +03:00]
3	Классификация инцидента операционной надежности	Код вида (направления) деятельности финансовой организации	O	-	Выбор одного значения из списка: Из классификатора «Классификатор инцидентов защиты информации и инцидентов операционной надежности, в разрезе видов деятельности кредитных организаций, некредитных финансовых организаций и субъектов национальной платежной системы и составляющих их технологических процессов», приведенного в приложении 11	При наличии кода вида (направления) деятельности финансовой организации первого и второго уровня они заполняются через «.», например: [Код 1].[Код 2]
4		Код технологического процесса	O	-	Выбор одного значения из списка: Из классификатора «Классификатор инцидентов защиты информации и инцидентов операционной надежности, в разрезе видов деятельности кредитных организаций, некредитных финансовых организаций и субъектов национальной платежной системы и составляющих их технологических процессов», приведенного в приложении 11 Перечень зависит от поля «Код вида (направления) деятельности финансовой организации»	-

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
5		Код источника риска	О	-	Выбор одного значения из списка: Из классификатора «Источники риска», приведенного в приложении 28	-
6		Код типа инцидента	О	-	Выбор одного значения из списка: Из классификатора «Классификатор инцидентов защиты информации и инцидентов операционной надежности, в разрезе видов деятельности кредитных организаций, некредитных финансовых организаций и субъектов национальной платежной системы и составляющих их технологических процессов», приведенного в приложении 11 Перечень зависит от поля «Код технологического процесса»	-
7		Код инцидента	О	-	Выбор одного значения из списка: Из классификатора «Классификатор инцидентов защиты информации и инцидентов операционной надежности, в разрезе видов деятельности кредитных организаций, некредитных финансовых организаций и субъектов национальной платежной системы и составляющих их технологических процессов», приведенного в приложении 11 Перечень зависит от поля «Код типа инцидента защиты информации»	-

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
8	Сведения об объекте информационной инфраструктуры (Блок заполняется отдельно для каждого объекта информационной инфраструктуры, который оказал влияние на простой или деградацию технологического процесса)	Код уровня объекта информационной инфраструктуры, который оказал влияние на простой или деградацию технологического процесса	О	-	Выбор одного значения из списка: Из классификатора «Типы объектов и субъектов», приведенного в приложении 28	-
9		Код типа объекта информационной инфраструктуры, который оказал влияние на простой или деградацию технологического процесса	О	-	Выбор одного значения из списка: Из классификатора «Типы объектов и субъектов», приведенного в приложении 28 Перечень зависит от поля «Код уровня объекта информационной инфраструктуры»	-
10		Описание объекта информационной инфраструктуры, который оказал влияние на простой или деградацию технологического процесса, в формате CPE	О	-	В формате, соответствующем рекомендациям Банка России, опубликованным на официальном сайте	-
11	Сведения об инциденте операционной надежности	Установленный организацией режим осуществления услуг	О	-	Указывается в формате {дней*часов} в квартал	Указывается общее количество дней и общее количество часов в отчетный квартал, во время которого произошел инцидент операционной надежности, рассчитанные в соответствии с установленным в организации режимом осуществления услуг

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
12	Связь с другими уведомлениями	Вид связанного уведомления	УО	Заполняется в случае направления ранее в Банк России уведомления, связанного с текущим	Выбор одного значения из списка: [NTF_OWC] [NTF_ISI] [NTF_ORI] [NTF_CI] [NTF_CA] [NTF_VLN]	[NTF_OWC] – уведомление о выявленных случаях и (или) попытках осуществления переводов денежных средств без согласия клиента, а также о выявленных случаях и (или) попытках осуществления операций, направленных на совершение финансовых сделок с использованием финансовой платформы без волеизъявления участника финансовой платформы [NTF_ISI] – уведомление о выявлении инцидента защиты информации или результатах расследования инцидента защиты информации [NTF_ORI] – уведомление о выявлении инцидента операционной надежности или о результатах расследования инцидента операционной надежности [NTF_CI] – уведомление о компьютерных инцидентах [NTF_CA] – уведомления о компьютерных атаках [NTF_VLN] – уведомление о выявленных уязвимостях»
13		Тип связи с другими уведомлениями			Выбор одного значения из списка: [Предшествующее событие] [Дочернее событие] [Связанное событие] [Уточнение сведений о событии]	-
14		Регистрационный номер уведомления			В соответствии с форматом АСОИ ФинЦЕРТ	Идентификатор уведомления или ответа на запрос, ранее направленного в ФинЦЕРТ участником информационного обмена
15	Ограничительный маркер TLP	Ограничительный маркер на распространение сведений из данного уведомления	Н	-	Выбор одного значения из списка: [TLP: WHITE] [TLP: GREEN] [TLP: AMBER] [TLP: RED]	В соответствии с обозначениями, принятыми в протоколе TLP По умолчанию [TLP: GREEN], если не указано иное

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
16	Необходимость привлечения ФинЦЕРТ	Необходимость привлечения ФинЦЕРТ	УО	При необходимости	[Да]	Необходимость привлечения ФинЦЕРТ для проведения расследования инцидента защиты информации, результаты которого должны быть направлены уведомлением о расследовании

ПРИЛОЖЕНИЕ 17. ФОРМА ПРЕДСТАВЛЕНИЯ ДАННЫХ NTF_ORI_INVESTIGATION – ФОРМА ПРЕДСТАВЛЕНИЯ УЧАСТНИКАМИ ИНФОРМАЦИОННОГО ОБМЕНА ДАННЫХ О РЕЗУЛЬТАТАХ РАССЛЕДОВАНИЯ ИНЦИДЕНТА ОПЕРАЦИОННОЙ НАДЕЖНОСТИ

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип уведомления	Тип уведомления	О	-	[NTF_ORI_Investigation]	Предзаполненное поле
2	Связь с уведомлением о выявлении инцидента операционной надежности	Идентификатор уведомления о выявлении инцидента операционной надежности	О	-	В соответствии с форматом АСОИ ФинЦЕРТ	Идентификатор уведомления или ответа на запрос, ранее направленного в ФинЦЕРТ участником информационного обмена
3	Дата и время	Дата и время фактического свершения инцидента операционной надежности	О	-	В соответствии с RFC 3339	По московскому времени [UTC +03:00]
4	Уточнение данных, содержащихся в уведомлении о выявлении инцидента операционной надежности	Код вида (направления) деятельности финансовой организации	УО	При необходимости уточнить классификацию инцидента операционной надежности, ранее предоставленную в уведомление о выявлении инцидента операционной надежности	Выбор одного значения из списка: Из классификатора «Классификатор инцидентов защиты информации и инцидентов операционной надежности, в разрезе видов деятельности кредитных организаций, некредитных финансовых организаций и субъектов национальной платежной системы и составляющих их технологических процессов», приведенного в приложении 11	При наличии кода вида (направления) деятельности финансовой организации первого и второго уровня они заполняются через «.», например: [Код 1].[Код 2]

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
5		Код технологического процесса			Выбор одного значения из списка: Из классификатора «Классификатор инцидентов защиты информации и инцидентов операционной надежности, в разрезе видов деятельности кредитных организаций, некредитных финансовых организаций и субъектов национальной платежной системы и составляющих их технологических процессов», приведенного в приложении 11 Перечень зависит от поля «Код вида (направления) деятельности финансовой организации»	-
6		Код источника риска			Выбор одного значения из списка: Из классификатора «Источники риска», приведенного в приложении 28	-
7		Код типа инцидента			Выбор одного значения из списка: Из классификатора «Классификатор инцидентов защиты информации и инцидентов операционной надежности, в разрезе видов деятельности кредитных организаций, некредитных финансовых организаций и субъектов национальной платежной системы и составляющих их технологических процессов», приведенного в приложении 11 Перечень зависит от поля «Код технологического процесса»	-

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
8		Код инцидента			Выбор одного значения из списка: Из классификатора «Классификатор инцидентов защиты информации и инцидентов операционной надежности, в разрезе видов деятельности кредитных организаций, некредитных финансовых организаций и субъектов национальной платежной системы и составляющих их технологических процессов», приведенного в приложении 11 Перечень зависит от поля «Код типа инцидента защиты информации»	-
9	«Сведения об объекте информационной инфраструктуры (блок заполняется отдельно для каждого объекта информационной инфраструктуры, который оказал влияние на простой или деградацию технологического процесса)	Код уровня объекта информационной инфраструктуры, который оказал влияние на простой или деградацию технологического процесса	УО	Блок заполняется в случае выявления объектов информационной инфраструктуры, которые оказали влияние на простой или деградацию технологического процесса, и не были направлены в уведомлении о выявлении инцидента операционной надежности	Выбор одного значения из списка: Из классификатора «Типы объектов и субъектов», приведенного в приложении 28	-
10		Код типа объекта информационной инфраструктуры, который оказал влияние на простой или деградацию технологического процесса			Выбор одного значения из списка: Из классификатора «Типы объектов и субъектов», приведенного в приложении 28 Перечень зависит от поля «Код уровня объекта/субъекта»	-
11		Описание объекта информационной инфраструктуры, который оказал влияние на простой или деградацию технологического процесса, в формате CPE			В формате, соответствующем рекомендациям Банка России, опубликованным на официальном сайте	-
12	Сведения об инциденте операционной надежности	Дата и время восстановления оказания услуг в полном объеме	О	-	В соответствии с RFC 3339	По московскому времени [UTC +03:00]

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
13		Фактическая доля деградации технологического процесса, на выполнение которого оказал влияние инцидент операционной надежности	О	-	Информация по показателю указывается в виде десятичной дроби с точностью до шести знаков после запятой (например, 0,000068)	Отношение общего количества операций, осуществляемых в рамках технологического процесса, совершенных во время деградации технологического процесса, в рамках инцидента операционной надежности, к ожидаемому количеству операций, осуществляемых в рамках технологического процесса, за тот же период в случае непрерывного оказания услуг
14		Фактическое время простоя и (или) деградации технологического процесса, на выполнение которого оказал влияние инцидент операционной надежности	О	-	В минутах	Указывается количество времени с момента начала простоя и (или) деградации технологического процесса, связанного с осуществлением услуг, до момента восстановления оказания услуг в полном объеме
15		Количество распоряжений, не выполненных в результате реализации инцидента	УО	При наличии информации в части количества распоряжений, не выполненных в результате реализации инцидента	Целое число >0	-
16		Сумма распоряжений, не выполненных в результате реализации инцидента			Сумма с точностью до двух знаков после запятой	-
17		Валюта			Из Общероссийского классификатора валют	-
18		Принятые меры	О	-	Текстовое поле	Текстовое описание принятых мер для нейтрализации и недопущения повторного инцидента
19	Ущерб от инцидента	Сумма прямых потерь	УО	Если такие потери являются последствиями реализации финансового инцидента и есть возможность их оценить	Сумма в рублях с точностью до двух знаков после запятой	К прямым потерям финансовой организации относятся потери, отраженные на счетах расходов и убытков в бухгалтерском учете и на приравненных к ним счетах по учету дебиторской задолженности

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
20		Сумма косвенных потерь	УО	Если такие потери являются последствиями реализации финансового инцидента и есть возможность их оценить	Сумма в рублях с точностью до двух знаков после запятой	Непрямые потери финансовой организации, не отраженные в бухгалтерском учете, но косвенно связанные с событиями риска реализации информационных угроз, включающие потери, определяемые расчетным методом в денежном выражении
21		Качественные потери	УО	Если на организацию распространяется требования об оценке таких потерь в соответствии с 716-П	В соответствии с критериями шкалы качественных оценок, установленной во внутренних документах организации	Непрямые потери финансовой организации, не отраженные в бухгалтерском учете, но косвенно связанные с событиями риска реализации информационных угроз, включающие потери, определяемые с использованием экспертного мнения, в случае если потери не выражены в денежном выражении расчетным методом
22		Сумма потенциальных потерь	УО	Если такие потери являются последствиями реализации финансового инцидента и есть возможность их оценить	Сумма в рублях с точностью до двух знаков после запятой	Непрямые потери финансовой организации, не отраженные в бухгалтерском учете, но косвенно связанные с событиями риска реализации информационных угроз, включающие потери, не реализовавшиеся в виде прямых и косвенных потерь, которые могли бы возникнуть при реализации не выявленных финансовой организацией источников риска реализации информационных угроз и (или) при неблагоприятном стечении обстоятельств
23		Мероприятия, осуществленные кредитной организацией в целях получения возмещения по понесенным потерям	УО	Если такие мероприятия проводились/проводятся	Текстовое поле	-
24	Уникальный порядковый идентификационный номер события операционного риска	Уникальный порядковый идентификационный номер события операционного риска в базе событий, соответствующего данному инциденту	УО	Только для кредитных организаций	Текстовое поле	-

ПРИЛОЖЕНИЕ 18. ПЕРЕЧЕНЬ КОМПЬЮТЕРНЫХ ИНЦИДЕНТОВ И КОМПЬЮТЕРНЫХ АТАК

Код компьютерного инцидента	Наименование компьютерного инцидента	Возможные векторы инцидента	Критерий информирования	Код компьютерной атаки	Наименование компьютерной атаки	Возможные векторы атаки	Критерий информирования
[DoS]	Замедление работы ресурса в результате атаки типа «Отказ в обслуживании»	[INT] – направлено на объекты информатизации финансовой организации	Выявлен факт осуществления DoS-атаки (в процессе или завершившейся) с полным или частичным прерыванием доступности или деградацией сервиса, используемого для проведения банковских или финансовых операций	[DoS]	Компьютерная атака типа «Отказ в обслуживании»	[INT] – направлено на объекты информатизации финансовой организации	В течение отчетного периода были выявлены попытки осуществления DoS-атаки (в процессе или завершившейся), если профиль объема трафика превышает показатели, установленные внутренними регламентами организации (в случае отсутствия такого показателя, вырос более чем в пять раз от обычного значения) и контролируемый ресурс продолжает функционировать в штатном режиме без деградации в производительности. Имеется информация об источниках вредоносной активности
[Application compromise]	Успешная эксплуатация уязвимости	[INT] – направлено на объекты информатизации финансовой организации	Зафиксирован факт успешной эксплуатации уязвимости на оборудовании или в программном обеспечении организации	[Exploit attempt]	Попытки эксплуатации уязвимости	[INT] – направлено на объекты информатизации финансовой организации	В течение отчетного периода были выявлены попытки эксплуатации уязвимостей на оборудовании или в программном обеспечении организации. Имеется информация об источниках вредоносной активности, а также описание эксплуатируемых уязвимостей в системе описания уязвимостей или сформировано экспертное мнение участника об уязвимости, не описанной ни в одной системе описания уязвимостей

Код компьютерного инцидента	Наименование компьютерного инцидента	Возможные векторы инцидента	Критерий информирования	Код компьютерной атаки	Наименование компьютерной атаки	Возможные векторы атаки	Критерий информирования
[Malware infection]	Заражение ВПО	[EXT] – направлено на клиента финансовой организации	Выявлен факт исполнения вредоносного кода на устройстве клиента, позволившее осуществить финансовую операцию без согласия клиента. Имеется образец вредоносного кода, его часть или подозрительный по мнению участника файл, который ранее не передавался в ФинЦЕРТ	[Infection attempt]	Попытки внедрения модулей ВПО	[EXT] – направлено на клиента финансовой организации	В течение отчетного периода были выявлены ресурсы в сети Интернет, содержащие вредоносный код или информацию, позволяющую осуществить неправомерный доступ к информационным системам участников информационного обмена и их клиентов, используемым при предоставлении (получении) финансовых услуг, в том числе путем неправомерного доступа к конфиденциальной информации клиентов
		[INT] – направлено на объекты информатизации финансовой организации	Выявлен факт исполнения вредоносного кода: – на рабочих станциях, ноутбуках, планшетах сотрудников, на которых осуществляется исполнение функциональных обязанностей; – на серверах и сетевом оборудовании организации; – на устройствах самообслуживания, станциях POS-терминалов и АТМ; – на ином оборудовании организации, на котором возможно исполнение вредоносного кода и компрометация которого по мнению участника может привести к ущербу организации			[INT] – направлено на объекты информатизации финансовой организации	В течение отчетного периода был обнаружен вредоносный код: – в теле сообщения электронной почты; – на рабочих станциях, ноутбуках, планшетах сотрудников, на которых осуществляется исполнение функциональных обязанностей; – на серверах и сетевом оборудовании организации; – на устройствах самообслуживания, станциях POS-терминалов и АТМ; – на ином оборудовании организации, на котором возможно детектирование вредоносного кода и компрометация которого по мнению участника может привести к ущербу организации. Имеется образец вредоносного кода, его часть или подозрительный по мнению участника файл, не направлявшийся ранее в ФинЦЕРТ

Код компьютерного инцидента	Наименование компьютерного инцидента	Возможные векторы инцидента	Критерий информирования	Код компьютерной атаки	Наименование компьютерной атаки	Возможные векторы атаки	Критерий информирования
[Account compromise]	Компрометация учетной записи	[EXT] – направлено на клиента финансовой организации	Выявлен факт компрометации аутентификационных данных (логинов-паролей) клиента, позволивший осуществить финансовую операцию без согласия клиента. Имеется информация об источниках компрометации учетных данных или источниках вредоносной активности	[Login attempt]	Неуспешные попытки авторизации	[EXT] – направлено на клиента финансовой организации	В течение отчетного периода были выявлены факты перебора аутентификационных данных (логинов-паролей), электронных почтовых адресов, папок сервера, URL различных веб-интерфейсов или зафиксирована попытка получения любых иных вышеуказанным методом данных. В ходе реагирования на атаку удалось установить, что перебор НЕ вызван ошибочными действиями легитимного пользователя, ошибками конфигурации или функционированием средств анализа защищенности, используемых участником. Количество неуспешных попыток перебора для одного логина превышает показатели, установленные внутренними регламентами организации (в случае отсутствия такого показателя, превышает 5 неуспешных попыток). Имеется информация об источниках вредоносной активности
		[INT] – направлено на объекты информатизации финансовой организации	Выявлен факт компрометации аутентификационных данных (логинов-паролей), электронных почтовых адресов, папок сервера, URL различных веб-интерфейсов			[INT] – направлено на объекты информатизации финансовой организации	
[Prohibited content]	Публикация на контролируемом ресурсе запрещенной законодательством РФ информации	[INT] – направлено на объекты информатизации финансовой организации	В контролируемом ресурсе выявлена информация, запрещенная законодательством РФ				

Код компьютерного инцидента	Наименование компьютерного инцидента	Возможные векторы инцидента	Критерий информирования	Код компьютерной атаки	Наименование компьютерной атаки	Возможные векторы атаки	Критерий информирования
[Traffic hijacking]	Захват сетевого трафика	[INT] – направлено на объекты информатизации финансовой организации	Выявлен факт изменения маршрутно-адресной информации. Инцидент актуален для тех финансовых организаций, которые содержат собственные AS, владеют собственными блоками IP-адресов и анонсируют их на бордерах операторов связи, арендуют IP-адреса либо разместили свои ресурсы в арендованой инфраструктуре, и атаки типа BGP-hijack были направлены по сути на «арендодателя»				
[Unauthorised modification]	Несанкционированное изменение информации	[INT] – направлено на объекты информатизации финансовой организации	Выявление факта несанкционированной модификации защищаемой информации, обрабатываемой в контролируемом ресурсе, или передаваемой по каналам связи				
[Unauthorised access]	Несанкционированное разглашение информации	[INT] – направлено на объекты информатизации финансовой организации	Выявление факта несанкционированного разглашения защищаемой («чувствительной») информации (например, код на гитхабе, в котором забыли удалить комментарии/логины-пароли), обрабатываемой в контролируемом ресурсе, или передаваемой по каналам связи				
[Attack using resource]	Использование контролируемого ресурса для проведения атак	[INT] – направлено на объекты информатизации финансовой организации	Выявлен факт использования контролируемого ресурса для проведения атак на другие объекты информационной инфраструктуры				
[Without attack]	Инцидент, не связанный с компьютерной атакой	[INT] – направлено на объекты информатизации финансовой организации	Выявлен факт нарушения или прекращения функционирования объекта КИИ или сети электросвязи, используемой для организации взаимодействия таких объектов, не связанный с компьютерной атакой на объект КИИ или сети электросвязи				

Код компьютерного инцидента	Наименование компьютерного инцидента	Возможные векторы инцидента	Критерий информирования	Код компьютерной атаки	Наименование компьютерной атаки	Возможные векторы атаки	Критерий информирования
[Social engineering]	Социальная инженерия	[EXT] – направлено на клиента финансовой организации	Успешная реализация атаки, направленная на клиентов организации или контрагентов, которая привела к финансовым потерям, утечки конфиденциальной информации или другим значимым последствиям, с использованием: – звонка с телефонного номера; – СМС-сообщения; – электронной почты; – систем мгновенного обмена сообщениями (мессенджерами); – иного канала взаимодействия с клиентами или контрагентами. Наличие информации, с использованием которой осуществлялось применение методов социальной инженерии, в том числе номер телефона, e-mail-адрес, технический заголовок письма, текст письма/СМС/сообщения системы мгновенных сообщений и т. д.	[Social engineering]	Попытки социальной инженерии	[EXT] – направлено на клиента финансовой организации [INT] – направлено на объекты информатизации финансовой организации	В течение отчетного периода были выявлены факты использования методов социальной инженерии в отношении работников организации, клиентов организации или контрагентов с использованием: – звонка с телефонного номера; – СМС-сообщения; – электронной почты; – систем мгновенного обмена сообщениями (мессенджерами); – иного канала обмена информацией внутри организации или взаимодействия с клиентами или контрагентами. Наличие информации, с использованием которой осуществлялось применение методов социальной инженерии, в том числе номер телефона, e-mail-адрес, технический заголовок письма, текст письма/СМС/сообщения системы мгновенных сообщений и т. д.
		[INT] – направлено на объекты информатизации финансовой организации	Успешная реализация атаки, направленная на работников организации, которая привела к финансовым потерям, утечки конфиденциальной информации или другим значимым последствиям, с использованием: – звонка с телефонного номера; – СМС-сообщения; – электронной почты; – систем мгновенного обмена сообщениями (мессенджерами); – иного канала обмена информацией внутри организации				
[SIM]	Изменение (подмена) идентификатора мобильного абонента (IMSI), идентификатора мобильного оборудования (IMEI) или сим-карты	[EXT] – направлено на клиента финансовой организации	Получение обращения (уведомления, заявления) клиента о проведении финансовой операции без его согласия с использованием сим-карты, которая была несанкционировано заменена				

Код компьютерного инцидента	Наименование компьютерного инцидента	Возможные векторы инцидента	Критерий информирования	Код компьютерной атаки	Наименование компьютерной атаки	Возможные векторы атаки	Критерий информирования
				[Phishing]	Выявление фишинговой рассылки или ресурса	[EXT] – направлено на клиента финансовой организации	В течение отчетного периода были выявлены ресурсы в сети Интернет, содержащие информацию, вводящую участников информационного обмена и их клиентов, а также иных взаимодействующих с ним лиц в заблуждение, вследствие сходства доменных имен, оформления и (или) содержания ресурса с оформлением и (или) содержанием официальных ресурсов участника, его клиентов, других участников, их клиентов или контрагентов. Наличие URL фишингового ресурса. Дополнительно выявлены промежуточные инфраструктурные элементы фишинговой инфраструктуры (промежуточные сервера для проксирования пользователя к фишинговой странице) или зарегистрированные, но еще не анонсированные доменные имена с признаками фишинга (хотя де-юре такое доменное имя как бы уже «опубликовано» в регистратуре ТЦИ и т. п.)
						[INT] – направлено на объекты информатизации финансовой организации	В течение отчетного периода были выявлены фишинговые сообщения, содержащие в электронном почтовом адресе отправителя в любом варианте написания слова «bank», «cbr», «fincert», "fsb», «fssp», «mvd», «pfrf», «npf», «gosuslugi», а также иные слова, схожие с наименованиями органов государственной власти, государственных автоматизированных систем, участников финансового рынка (согласно техническим заголовкам не может быть отправлено с легитимного почтового адреса). Наличие источников фишинговой рассылки

Код компьютерного инцидента	Наименование компьютерного инцидента	Возможные векторы инцидента	Критерий информирования	Код компьютерной атаки	Наименование компьютерной атаки	Возможные векторы атаки	Критерий информирования
				[Scanning]	Сетевое сканирование контролируемого ресурса	[INT] – направлено на объекты информатизации финансовой организации	В течение отчетного периода были выявлены факты сканирования контролируемых ресурсов и если профиль объема трафика сканирования превышает показатели, установленные внутренними регламентами организации (в случае отсутствия такого показателя, вырос в пять раз от обычного значения). Наличие сведений об источниках сканирования

ПРИЛОЖЕНИЕ 19. ФОРМА ПРЕДСТАВЛЕНИЯ ДАННЫХ NTF_CI – ФОРМА ПРЕДСТАВЛЕНИЯ УЧАСТНИКАМИ ИНФОРМАЦИОННОГО ОБМЕНА ДАННЫХ О КОМПЬЮТЕРНЫХ ИНЦИДЕНТАХ

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип уведомления	Тип уведомления	О	-	[NTF_CI]	Предзаполненное поле
2	Описание компьютерного инцидента	Описание компьютерного инцидента	Н	-	Текстовое поле	Текстовое описание компьютерного инцидента (в том числе дополнительные сведения о способе реализации КИ, способе выявления КИ и т. д.). В случае если компьютерный инцидент был выявлен с использованием сведений бюллетеня Банка России или НКЦКИ, необходимо указать номер данного бюллетеня
3	Классификация компьютерного инцидента	Вектор	О	-	[EXT] [INT]	В соответствии с классификатором компьютерных инцидентов, приведенным в приложении 18
4		Тип компьютерного инцидента	О	-	[DoS] [Application compromise] [Malware infection] [Account compromise] [Prohibited content] [Social engineering] [Traffic hijacking] [Unauthorised modification] [Unauthorised access] [SIM] [Attack using resource] [Without attack]	В соответствии с классификатором компьютерных инцидентов, приведенным в приложении 18
5	Дата и время обнаружения	Дата и время выявления компьютерного инцидента	О	-	В соответствии с RFC 3339	По московскому времени [UTC +03:00]
6	Сведения об объектах, на которые направлен компьютерный инцидент	Набор данных	УО	Состав данных зависит от поля «Тип компьютерного инцидента» и приведен на вкладке «Сведения об объектах КИ»		-
7	Сведения об объектах вредоносной активности, вызвавших компьютерный инцидент	Набор данных	УО	Состав данных зависит от поля «Тип компьютерного инцидента» и приведен на вкладке «Сведения об объектах ВА»		-
8	Сведения о незаконном раскрытии ПДн	Предполагаемые причины, повлекшие нарушение прав субъектов ПДн	УО	Блок заполняется в случае, если в результате компьютерного инцидента произошла утечка ПДн	Текстовое поле	Описание событий, которые привели к незаконному раскрытию информации. Поле заполняется, если в поле «Описание компьютерного инцидента» недостаточно информации о незаконном раскрытии ПДн

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
9		Характеристики ПДн			Текстовое поле	Указывается информация характеризующая незаконно раскрытые ПДн, в том числе тип субъекта, чьи ПДн были раскрыты, состав незаконно раскрытых ПДн, количество и актуальность записей и т. д.
10		Предполагаемый вред, нанесенный правам субъектов ПДн			Текстовое поле	Описание потенциального вреда, который может быть нанесен субъектам при использовании незаконно раскрытой информации
11		ФИО лица, уполномоченного оператором на взаимодействие с Роскомнадзором по инциденту			Текстовое поле	-
12		Мобильный телефон лица, уполномоченного на взаимодействие с Роскомнадзором по инциденту			В соответствии с российской системой и планом нумерации	-
13		Адрес электронной почты для отправки информации об уведомлении			В формате e-mail-адреса	-
14	Оценка последствий компьютерного инцидента	Влияние на конфиденциальность	УО	При наличии указанных последствий	[Высокое] [Низкое]	-
15		Влияние на целостность			[Высокое] [Низкое]	-
16		Влияние на доступность			[Высокое] [Низкое]	-
17	Предпринятые меры по реагированию на компьютерный инцидент	Описание предпринятых действий в ходе реагирования на компьютерный инцидент	Н	-	Текстовое поле	-

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
18	Связь с другими уведомлениями	Вид связанного уведомления	УО	Заполняется в случае направления ранее в Банк России уведомления, связанного с текущим	[NTF_OWC] [NTF_ISI] [NTF_ORI] [NTF_CI] [NTF_CA] [NTF_VLN]	[NTF_OWC] – уведомление о выявленных случаях и (или) попытках осуществления переводов денежных средств без согласия клиента, а также о выявленных случаях и (или) попытках осуществления операций, направленных на совершение финансовых сделок с использованием финансовой платформы без волеизъявления участника финансовой платформы [NTF_ISI] – уведомление о выявлении инцидента защиты информации или результатах расследования инцидента защиты информации [NTF_ORI] – уведомление о выявлении инцидента операционной надежности или о результатах расследования инцидента операционной надежности [NTF_CI] – уведомление о компьютерных инцидентах [NTF_CA] – уведомления о компьютерных атаках [NTF_VLN] – уведомление о выявленных уязвимостях
19		Тип связи с другими уведомлениями			[Предшествующее событие] [Дочернее событие] [Связанное событие] [Уточнение сведений о событии]	-
20		Регистрационный номер уведомления			В соответствии с форматом АСОИ ФинЦЕРТ	Идентификатор уведомления или ответа на запрос, ранее направленного в ФинЦЕРТ участником информационного обмена
21	Ограничительный маркер TLP	Ограничительный маркер на распространение сведений из данного уведомления	Н	-	[TLP: WHITE] [TLP: GREEN] [TLP: AMBER] [TLP: RED]	В соответствии с обозначениями, принятыми в протоколе TLP. По умолчанию [TLP: GREEN], если не указано иное
22	Необходимость привлечения ФинЦЕРТ	Необходимость привлечения ФинЦЕРТ для устранения последствий компьютерного инцидента	УО	При необходимости	[Да]	-

Код компьютерного инцидента	Наименование компьютерного инцидента	Технические сведения об объектах, на которые направлен компьютерный инцидент				
		Описание АСОИ UI	**Обязательность полей**	**Условие обязательности**	**Правило заполнения**	**Примечание**
[DoS]	Замедление работы ресурса в результате атаки типа «Отказ в обслуживании»	Наименование контролируемого ресурса	О	-	Текстовое поле	-
		Категория контролируемого ресурса	УО	Если является объектом КИИ	[Без категории значимости] [Третья категория значимости] [Вторая категория значимости] [Первая категория значимости]	-
		Код уровня объекта/субъекта	О	-	Из классификатора «Типы объектов и субъектов», приведенного в приложении 28	-
		Код типа объекта/субъекта	О	-	Перечень зависит от поля «Код уровня атакуемого объекта/субъекта». Из классификатора «Типы объектов и субъектов», приведенного в приложении 28	-
		Наличие подключения к сети Интернет	О	-	[Да]	Предзаполненное поле
		Страна/регион	О	-	В формате ISO-3166-2	-
		IPv4-адрес контролируемого ресурса	УО	Обязательно заполнение одного из полей	Список IP-адресов	-
		IPv6-адрес контролируемого ресурса				
		Доменное имя контролируемого ресурса			Список доменных имен	
		URI-адрес контролируемого ресурса			Список URI-адресов	
		Атакованная сетевая служба и порт/протокол	УО	При наличии соответствующей информации	Текстовое поле	-
[Application compromise]	Успешная эксплуатация уязвимости	Наименование контролируемого ресурса	О	-	Текстовое поле	-
		Категория контролируемого ресурса	УО	Если является объектом КИИ	[Без категории значимости] [Третья категория значимости] [Вторая категория значимости] [Первая категория значимости]	-
		Код уровня объекта/субъекта	О	-	Из классификатора «Типы объектов и субъектов», приведенного в приложении 28	-

Код компьютерного инцидента	Наименование компьютерного инцидента	Технические сведения об объектах, на которые направлен компьютерный инцидент				
		Описание АСОИ UI	**Обязательность полей**	**Условие обязательности**	**Правило заполнения**	**Примечание**
		Код типа объекта/субъекта	О	-	Перечень зависит от поля «Код уровня атакуемого объекта/субъекта». Из классификатора «Типы объектов и субъектов», приведенного в приложении 28	-
		Наличие подключения к сети Интернет	О	-	[Да]/[Нет]	-
		Страна/регион	О	-	В формате ISO-3166-2	-
		IPv4-адрес контролируемого ресурса	УО	Обязательно заполнение одного из полей	Список IP-адресов	-
		IPv6-адрес контролируемого ресурса				
		Доменное имя контролируемого ресурса			Список доменных имен	
		URI-адрес контролируемого ресурса			Список URI-адресов	
		Атакованная сетевая служба и порт/протокол	УО	При наличии соответствующей информации	Текстовое поле	-
[Malware infection]	Заражение ВПО	Наименование контролируемого ресурса	О	-	Текстовое поле	-
		Категория контролируемого ресурса	УО	Если является объектом КИИ	[Без категории значимости] [Третья категория значимости] [Вторая категория значимости] [Первая категория значимости]	-
		Код уровня объекта/субъекта	О	-	Из классификатора «Типы объектов и субъектов», приведенного в приложении 28	-
		Код типа объекта/субъекта	О	-	Перечень зависит от поля «Код уровня атакуемого объекта/субъекта». Из классификатора «Типы объектов и субъектов», приведенного в приложении 28	-
		Наличие подключения к сети Интернет	О	-	[Да]/[Нет]	-
		Страна/регион	О	-	В формате ISO-3166-2	-
		IPv4-адрес контролируемого ресурса	УО	Обязательно заполнение одного из полей	Список IP-адресов	-
		IPv6-адрес контролируемого ресурса				
		Доменное имя контролируемого ресурса			Список доменных имен	
		URI-адрес контролируемого ресурса			Список URI-адресов	
		e-mail-адрес контролируемого объекта			Список e-mail-адресов	

Код компьютерного инцидента	Наименование компьютерного инцидента	Технические сведения об объектах, на которые направлен компьютерный инцидент				
		Описание АСОИ UI	**Обязательность полей**	**Условие обязательности**	**Правило заполнения**	**Примечание**
		Атакованная сетевая служба и порт/протокол	УО	При наличии соответствующей информации	Текстовое поле	-
[Account compromise]	Компрометация учетной записи	Наименование контролируемого ресурса	О	-	Текстовое поле	-
		Категория контролируемого ресурса	УО	Если является объектом КИИ	[Без категории значимости] [Третья категория значимости] [Вторая категория значимости] [Первая категория значимости]	-
		Код уровня объекта/субъекта	О	-	Из классификатора «Типы объектов и субъектов», приведенного в приложении 28	-
		Код типа объекта/субъекта	О	-	Перечень зависит от поля «Код уровня атакуемого объекта/субъекта». Из классификатора «Типы объектов и субъектов», приведенного в приложении 28	-
		Наличие подключения к сети Интернет	О	-	[Да]/[Нет]	-
		Страна/регион	О	-	В формате ISO-3166-2	-
		IPv4-адрес контролируемого ресурса	УО	Обязательно заполнение одного из полей	Список IP-адресов	-
		IPv6-адрес контролируемого ресурса				
		Доменное имя контролируемого ресурса			Список доменных имен	
		URI-адрес контролируемого ресурса			Список URI-адресов	
		e-mail-адрес контролируемого объекта			Список e-mail-адресов	
		Атакованная сетевая служба и порт/протокол	УО	При наличии соответствующей информации	Текстовое поле	-
[Prohibited content]	Публикация на контролируемом ресурсе запрещенной законодательством РФ информации	Наименование контролируемого ресурса	О	-	Текстовое поле	-
		Категория контролируемого ресурса	УО	Если является объектом КИИ	[Без категории значимости] [Третья категория значимости] [Вторая категория значимости] [Первая категория значимости]	-
		Код уровня объекта/субъекта	О	-	Из классификатора «Типы объектов и субъектов», приведенного в приложении 28	-

Код компьютерного инцидента	Наименование компьютерного инцидента	Технические сведения об объектах, на которые направлен компьютерный инцидент				
		Описание АСОИ UI	**Обязательность полей**	**Условие обязательности**	**Правило заполнения**	**Примечание**
		Код типа объекта/субъекта	О	-	Перечень зависит от поля «Код уровня атакуемого объекта/субъекта». Из классификатора «Типы объектов и субъектов», приведенного в приложении 28	-
		Наличие подключения к сети Интернет	О	-	[Да]/[Нет]	-
		Страна/регион	О	-	В формате ISO-3166-2	-
		IPv4-адрес контролируемого ресурса	УО	Обязательно заполнение одного из полей	Список IP-адресов	-
		IPv6-адрес контролируемого ресурса				
		Доменное имя контролируемого ресурса			Список доменных имен	
		URI-адрес контролируемого ресурса			Список URI-адресов	
[Traffic hijacking]	Захват сетевого трафика	Наименование контролируемого ресурса	О	-	Текстовое поле	-
		Категория контролируемого ресурса	УО	Если является объектом КИИ	[Без категории значимости] [Третья категория значимости] [Вторая категория значимости] [Первая категория значимости]	-
		Код уровня объекта/субъекта	О	-	Из классификатора «Типы объектов и субъектов», приведенного в приложении 28	-
		Код типа объекта/субъекта	О	-	Перечень зависит от поля «Код уровня атакуемого объекта/субъекта». Из классификатора «Типы объектов и субъектов», приведенного в приложении 28	-
		Наличие подключения к сети Интернет	О	-	[Да]/[Нет]	-
		Страна/регион	О	-	В формате ISO-3166-2	-
		AS-Path до контролируемой автономной системы (ASN)	О	-	Текстовое поле	-
[Unauthorised modification]	Несанкционированное изменение информации	Наименование контролируемого ресурса	О	-	Текстовое поле	-
		Категория контролируемого ресурса	УО	Если является объектом КИИ	[Без категории значимости] [Третья категория значимости] [Вторая категория значимости] [Первая категория значимости]	-

Код компьютерного инцидента	Наименование компьютерного инцидента	Технические сведения об объектах, на которые направлен компьютерный инцидент				
		Описание АСОИ UI	**Обязательность полей**	**Условие обязательности**	**Правило заполнения**	**Примечание**
		Код уровня объекта/субъекта	О	-	Из классификатора «Типы объектов и субъектов», приведенного в приложении 28	-
		Код типа объекта/субъекта	О	-	Перечень зависит от поля «Код уровня атакуемого объекта/субъекта». Из классификатора «Типы объектов и субъектов», приведенного в приложении 28	-
		Наличие подключения к сети Интернет	О	-	[Да]/[Нет]	-
		Страна/регион	О	-	В формате ISO-3166-2	-
		IPv4-адрес контролируемого ресурса	УО	Обязательно заполнение одного из полей	Список IP-адресов	-
		IPv6-адрес контролируемого ресурса				
		Доменное имя контролируемого ресурса			Список доменных имен	
		URI-адрес контролируемого ресурса			Список URI-адресов	
		Атакованная сетевая служба и порт/протокол	УО	При наличии соответствующей информации	Текстовое поле	-
[Unauthorised access]	Несанкционированное разглашение информации	Наименование контролируемого ресурса	О	-	Текстовое поле	-
		Категория контролируемого ресурса	УО	Если является объектом КИИ	[Без категории значимости] [Третья категория значимости] [Вторая категория значимости] [Первая категория значимости]	-
		Код уровня объекта/субъекта	О	-	Из классификатора «Типы объектов и субъектов», приведенного в приложении 28	-
		Код типа объекта/субъекта	О	-	Перечень зависит от поля «Код уровня атакуемого объекта/субъекта». Из классификатора «Типы объектов и субъектов», приведенного в приложении 28	-
		Наличие подключения к сети Интернет	О	-	[Да]/[Нет]	-
		Страна/регион	О	-	В формате ISO-3166-2	-
		IPv4-адрес контролируемого ресурса	УО	Обязательно заполнение одного из полей	Список IP-адресов	-
		IPv6-адрес контролируемого ресурса				
		Доменное имя контролируемого ресурса			Список доменных имен	

Код компьютерного инцидента	Наименование компьютерного инцидента	Технические сведения об объектах, на которые направлен компьютерный инцидент				
		Описание АСОИ UI	**Обязательность полей**	**Условие обязательности**	**Правило заполнения**	**Примечание**
		URI-адрес контролируемого ресурса			Список URI-адресов	
		e-mail-адрес контролируемого объекта			Список e-mail-адресов	
		Атакованная сетевая служба и порт/протокол	УО	При наличии соответствующей информации	Текстовое поле	-
[Social engineering]	Социальная инженерия	Код уровня объекта/субъекта	О	-	[Subject]	Предзаполненное поле
		Код типа объекта/субъекта	О	-	[Employee] [Client] [Partner]	Из классификатора «Тип атакуемого объекта-субъекта»
[SIM]	Изменение (подмена) идентификатора мобильного абонента (IMSI), идентификатора мобильного оборудования (IMEI) или сим-карты	-				
[Attack using resource]	Использование контролируемого ресурса для проведения атак	Наименование контролируемого ресурса	О	-	Текстовое поле	-
		Категория контролируемого ресурса	УО	Если является объектом КИИ	[Без категории значимости] [Третья категория значимости] [Вторая категория значимости] [Первая категория значимости]	-
		Код уровня объекта/субъекта	О	-	Из классификатора «Типы объектов и субъектов», приведенного в приложении 28	-
		Код типа объекта/субъекта	О	-	Перечень зависит от поля «Код уровня атакуемого объекта/субъекта». Из классификатора «Типы объектов и субъектов», приведенного в приложении 28	-
		Наличие подключения к сети Интернет	О	-	[Да]	Предзаполненное поле
		Страна/регион	О	-	В формате ISO-3166-2	-
		IPv4-адрес контролируемого ресурса	УО	Обязательно заполнение одного из полей	Список IP-адресов	-
		IPv6-адрес контролируемого ресурса				
		Доменное имя контролируемого ресурса			Список доменных имен	
		URI-адрес контролируемого ресурса			Список URI-адресов	
		e-mail-адрес контролируемого объекта			Список e-mail-адресов	
		Атакованная сетевая служба и порт/протокол	УО	При наличии соответствующей информации	Текстовое поле	-

Код компьютерного инцидента	Наименование компьютерного инцидента	Технические сведения об объектах, на которые направлен компьютерный инцидент				
		Описание АСОИ UI	**Обязательность полей**	**Условие обязательности**	**Правило заполнения**	**Примечание**
[Without attack]	Инцидент, не связанный с компьютерной атакой	Наименование контролируемого ресурса	О	-	Текстовое поле	-
		Категория контролируемого ресурса	УО	Если является объектом КИИ	[Без категории значимости] [Третья категория значимости] [Вторая категория значимости] [Первая категория значимости]	-
		Код уровня объекта/субъекта	О	-	Из классификатора «Типы объектов и субъектов», приведенного в приложении 28	-
		Код типа объекта/субъекта	О	-	Перечень зависит от поля «Код уровня атакуемого объекта/субъекта». Из классификатора «Типы объектов и субъектов», приведенного в приложении 28	-
		Наличие подключения к сети Интернет	О	-	[Да]/[Нет]	-
		Страна/регион	О	-	В формате ISO-3166-2	-
		IPv4-адрес контролируемого ресурса	УО	Обязательно заполнение одного из полей	Список IP-адресов	-
		IPv6-адрес контролируемого ресурса				
		Доменное имя контролируемого ресурса			Список доменных имен	
		URI-адрес контролируемого ресурса			Список URI-адресов	
		e-mail-адрес контролируемого объекта			Список e-mail-адресов	

Код компьютерного инцидента	Наименование компьютерного инцидента	Сведения об объектах или субъектах вредоносной активности, вызвавших компьютерный инцидент				
		Описание АСОИ UI	**Обязательность полей**	**Условие обязательности**	**Правило заполнения**	**Примечание**
[DoS]	Замедление работы ресурса в результате атаки типа «Отказ в обслуживании»	Тип атаки	О	-	[DoS – Flood] [DoS – Vuln] [DDos]	-
		Уровень OSI	О	-	[L2/3] [L3] [L4] [L6] [L7]	[L2/3] – канальный/сетевой уровень [L3] – сетевой уровень [L4] – транспортный уровень [L6] – уровень представления данных [L7] – прикладной уровень
		IPv4-адрес вредоносного объекта	УО	Выявлен IPv4-адрес вредоносного объекта	Список IP-адресов или csv-файл	Заполняется хотя бы одно поле
		IPv6-адрес вредоносного объекта		Выявлен IPv6-адрес вредоносного объекта		
		Доменное имя вредоносного объекта	УО	Выявлено доменное имя вредоносного объекта	Список доменных имен или csv-файл	
		Страна расположения вредоносного объекта	Н	-	Список трехбуквенных кодов стран в соответствии с ISO 3166	-
		PPS (пакетов в секунду)	УО	Заполняется хотя бы одно поле	Вещественное число	-
		Мб/с (мегабит в секунду)			Вещественное число	-
		RPS (запросов в секунду)			Вещественное число	-
		FPS (кадров в секунду)			Вещественное число	-
		Перечень используемых уязвимостей	УО	Выявлен факт использования уязвимостей	-	Перечень используемых уязвимостей программного или аппаратного обеспечения в выбранной системе описания уязвимостей безопасности (например, CVE, БДУ ФСТЭК)
		Наименование системы описания уязвимостей безопасности			Текстовое поле	
[Application compromise]	Успешная эксплуатация уязвимости	IPv4-адрес вредоносного объекта	УО	Выявлен IPv4-адрес вредоносного объекта	Список IP-адресов	-
		IPv6-адрес вредоносного объекта		Выявлен IPv6-адрес вредоносного объекта		-
		Доменное имя вредоносного объекта		Выявлено доменное имя вредоносного объекта	Список доменных имен	-
		URI-адрес вредоносного объекта		Выявлен URI-адрес вредоносного объекта	Список URI-адресов	-
		e-mail-адрес вредоносного объекта или субъекта		Выявлен e-mail-адрес вредоносного объекта или субъекта	Список e-mail-адресов	-
		Уязвимость	УО	В случае если выявленная уязвимость описана в какой-либо системе описания уязвимостей	Перечень эксплуатируемых уязвимостей безопасности программного или аппаратного обеспечения, из соответствующего каталога (например, CVE, БДУ ФСТЭК и т. д.)	Обязательно заполняется один из блоков

Код компьютерного инцидента	Наименование компьютерного инцидента	Сведения об объектах или субъектах вредоносной активности, вызвавших компьютерный инцидент				
		Описание АСОИ UI	**Обязательность полей**	**Условие обязательности**	**Правило заполнения**	**Примечание**
		Наименование системы описания уязвимостей			Текстовое поле	
		Описание уязвимости	УО	В случае если выявленная уязвимость не описана ни в одной системе описания уязвимостей	Текстовое поле	
		Описание объекта информатизации, в котором была проэксплуатирована уязвимость	О	-	В формате, соответствующем рекомендациям Банка России, опубликованными на официальном сайте	-
[Malware infection]	Заражение ВПО	IPv4-адрес вредоносного объекта	УО	Выявлен IPv4-адрес вредоносного объекта	Список IP-адресов	-
		IPv6-адрес вредоносного объекта		Выявлен IPv6-адрес вредоносного объекта		-
		Доменное имя вредоносного объекта		Выявлено доменное имя вредоносного объекта	Список доменных имен	-
		URI-адрес вредоносного объекта		Выявлен URI-адрес вредоносного объекта	Список URI-адресов	-
		e-mail-адрес вредоносного объекта или субъекта		Выявлен e-mail-адрес вредоносного объекта или субъекта	Список e-mail-адресов	-
		Название антивируса, выявившего заражение ВПО	УО	Если ВПО было выявлено антивирусом	Текстовое поле	-
		Описание и классификация вредоносного ПО	Н	-	Текстовое поле	-
		Сетевая активность	УО	При наличии информации о сетевой активности ВПО	Текстовое поле	-
		Уязвимость	УО	В случае если выявлен факт эксплуатации уязвимостей ВПО	Перечень эксплуатируемых уязвимостей безопасности программного или аппаратного обеспечения, из соответствующего каталога (например, CVE, БДУ ФСТЭК и т. д.)	-
		Наименование системы описания уязвимостей			Текстовое поле	-
		Описание уязвимости, не описанной ни в одной системе описания уязвимостей			Текстовое поле	-
		Файл ВПО	УО	Обязательно заполняется одно из полей	Файл	-
		URL для скачивания			Текстовое поле	-
		Хеш-сумма	О	-	Текстовое поле	-
		Алгоритм хеширования		-	[SHA256] [SHA1] [MD5]	-

Код компьютерного инцидента	Наименование компьютерного инцидента	Сведения об объектах или субъектах вредоносной активности, вызвавших компьютерный инцидент				
		Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
[Account compromise]	Компрометация учетной записи	IPv4-адрес вредоносного объекта	УО	Выявлен IPv4-адрес вредоносного объекта	Список IP-адресов	-
		IPv6-адрес вредоносного объекта		Выявлен IPv6-адрес вредоносного объекта		-
		Доменное имя вредоносного объекта		Выявлено доменное имя вредоносного объекта	Список доменных имен	-
		Логин скомпрометированной УЗ	О	-	Текстовое поле	-
		Привилегии скомпрометированной УЗ	О	-	Текстовое поле	-
		Способ компрометации	УО	При наличии соответствующей информации	Текстовое поле	-
[Prohibited content]	Публикация на контролируемом ресурсе запрещенной законодательством РФ информации	IPv4-адрес вредоносного объекта	УО	Выявлен IPv4-адрес вредоносного объекта	Список IP-адресов	-
		IPv6-адрес вредоносного объекта		Выявлен IPv6-адрес вредоносного объекта		-
		Доменное имя вредоносного объекта		Выявлено доменное имя вредоносного объекта	Список доменных имен	-
		URI-адрес вредоносного объекта		Выявлен URI-адрес вредоносного объекта	Список URI-адресов	-
[Traffic hijacking]	Захват сетевого трафика	Номер подставной автономной системы (ASN)	О	-	Текстовое поле	-
		Наименование AS	О	-	Текстовое поле	-
		Наименование LIR	О	-	Текстовое поле	-
		Ссылка на Looking Glass	УО	При наличии	Текстовое поле	-
		Штатный prefix	Н	-	Текстовое поле	-
		Подставной prefix	Н	-	Текстовое поле	-
[Unauthorised modification]	Несанкционированное изменение информации	IPv4-адрес вредоносного объекта	УО	Выявлен IPv4-адрес вредоносного объекта	Список IP-адресов	-
		IPv6-адрес вредоносного объекта		Выявлен IPv6-адрес вредоносного объекта		-
		Доменное имя вредоносного объекта		Выявлено доменное имя вредоносного объекта	Список доменных имен	-
		URI-адрес вредоносного объекта		Выявлен URI-адрес вредоносного объекта	Список URI-адресов	-
[Unauthorised access]	Несанкционированное разглашение информации	IPv4-адрес вредоносной системы	УО	Выявлен IPv4-адрес вредоносной системы или объекта	Список IP-адресов	-
		IPv6-адрес вредоносной системы		Выявлен IPv6-адрес вредоносной системы или объекта		-
		Доменное имя вредоносной системы		Выявлено доменное имя вредоносной системы или объекта	Список доменных имен	-

Код компьютерного инцидента	Наименование компьютерного инцидента	Сведения об объектах или субъектах вредоносной активности, вызвавших компьютерный инцидент				
		Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
		e-mail-адрес вредоносного объекта		Выявлен e-mail-адрес вредоносной системы или объекта	Список e-mail-адресов	-
[Social engineering]	Социальная инженерия	IPv4-адрес вредоносного объекта	УО	Выявлен IPv4-адрес вредоносного объекта	Список IP-адресов	-
		IPv6-адрес вредоносного объекта		Выявлен IPv6-адрес вредоносного объекта		-
		Доменное имя вредоносного объекта		Выявлено доменное имя вредоносного объекта	Список доменных имен	-
		URI-адрес вредоносного объекта		Выявлен URI-адрес вредоносного объекта	Список URI-адресов	-
		e-mail-адрес вредоносного объекта или субъекта		Выявлен e-mail-адрес вредоносного объекта или субъекта	Список e-mail-адресов	-
		Абонентский номер подвижной радиотелефонной связи вредоносного субъекта		Выявлен номер мобильного телефона вредоносного субъекта	Список номеров мобильных телефонов в соответствии с российской системой и планом нумерации	-
		Канал взаимодействия	О	-	[Телефонный звонок] [СМС] [Электронная почта] [Система обмена мгновенными сообщениями] [Сайт] [Иной канал]	-
		Текст сообщения	УО	«Канал взаимодействия» = { [СМС], [Электронная почта], [Система обмена мгновенными сообщениями]}	Тестовое поле или txt-файл	-
[SIM]	Изменение (подмена) идентификатора мобильного абонента (IMSI), идентификатора мобильного оборудования (IMEI) или сим-карты	Абонентский номер подвижной радиотелефонной связи	О	-	В соответствии с российской системой и планом нумерации	-
		IMSI	О	-	Текстовое поле	-
		Оператор связи	Н	-	Текстовое поле	-
		Дата смены IMSI	Н	-	В соответствии с RFC 3339	По московскому времени [UTC +03:00]
[Attack using resource]	Использование контролируемого ресурса для проведения атак	IPv4-адрес вредоносного объекта	УО	Выявлен IPv4-адрес вредоносного объекта	Список IP-адресов	-
		IPv6-адрес вредоносного объекта		Выявлен IPv6-адрес вредоносного объекта		-
		Доменное имя вредоносного объекта		Выявлено доменное имя вредоносного объекта	Список доменных имен	-

Код компьютерного инцидента	Наименование компьютерного инцидента	Сведения об объектах или субъектах вредоносной активности, вызвавших компьютерный инцидент				
		Описание АСОИ UI	**Обязательность полей**	**Условие обязательности**	**Правило заполнения**	**Примечание**
		URI-адрес вредоносного объекта		Выявлен URI-адрес вредоносного объекта	Список URI-адресов	-
		e-mail-адрес вредоносного объекта или субъекта		Выявлен e-mail-адрес вредоносного объекта или субъекта	Список e-mail-адресов	-
		Уязвимость	УО	В случае если выявленная уязвимость описана в какой-либо системе описания уязвимостей	Перечень эксплуатируемых уязвимостей безопасности программного или аппаратного обеспечения, из соответствующего каталога (например, CVE, БДУ ФСТЭК и т. д.)	Обязательно заполняется один из блоков
		Наименование системы описания уязвимостей			Текстовое поле	
		Описание уязвимости	УО	В случае если выявленная уязвимость не описана ни в одной системе описания уязвимостей	Текстовое поле	
		Описание объекта информатизации, в котором была проэксплуатирована уязвимость	О	-	В формате, соответствующем рекомендациям Банка России, опубликованными на официальном сайте	-
		Файл ВПО	УО	Обязательно заполняется одно из полей	Файл	-
		URL для скачивания			Текстовое поле	-
		Хеш-сумма	О	-	Текстовое поле	-
		Алгоритм хеширования		-	[SHA256] [SHA1] [MD5]	-
[Without attack]	Инцидент, не связанный с компьютерной атакой	-				

ПРИЛОЖЕНИЕ 20. ФОРМЫ ПРЕДСТАВЛЕНИЯ ДАННЫХ NTF_CI, ПРЕДЗАПОЛНЕННЫЕ ДЛЯ КОМПЬЮТЕРНЫХ ИНЦИДЕНТОВ

Код компьютерного инцидента	Наименование компьютерного инцидента
[DoS]	Замедление работы ресурса в результате атаки типа «Отказ в обслуживании»
[Application compromise]	Успешная эксплуатация уязвимости
[Malware infection]	Заражение ВПО
[Account compromise]	Компрометация учетной записи
[Prohibited content]	Публикация на контролируемом ресурсе запрещенной законодательством РФ информации
[Social engineering]	Социальная инженерия
[Traffic hijacking]	Захват сетевого трафика
[Unauthorised modification]	Несанкционированное изменение информации
[Unauthorised access]	Несанкционированное разглашение информации
[SIM]	Изменение (подмена) идентификатора мобильного абонента (IMSI), идентификатора мобильного оборудования (IMEI) или сим-карты
[Attack using resource]	Использование контролируемого ресурса для проведения атак
[Without attack]	Инцидент, не связанный с компьютерной атакой

Форма представления данных NTF_CI_DoS – Форма представления данных о компьютерном инциденте, связанном с замедлением работы ресурса в результате атаки типа «Отказ в обслуживании»

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип уведомления	Тип уведомления	O	-	[NTF_CI_DoS]	Предзаполненное поле
2	Описание компьютерного инцидента	Описание компьютерного инцидента	H	-	Текстовое поле	Текстовое описание компьютерного инцидента (в том числе дополнительные сведения о способе реализации КИ, способе выявления КИ и т. д.). В случае если компьютерный инцидент был выявлен с использованием сведений бюллетеня Банка России или НКЦКИ, необходимо указать номер данного бюллетеня
3	Классификация компьютерного инцидента	Вектор	O	-	[INT]	Предзаполненное поле
4		Тип компьютерного инцидента	O	-	[DoS]	Предзаполненное поле
5	Дата и время обнаружения	Дата и время выявления компьютерного инцидента	O	-	В соответствии с RFC 3339	По московскому времени [UTC +03:00]

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
6	Сведения об объектах, на которые направлен компьютерный инцидент	Наименование контролируемого информационного ресурса	О	-	Текстовое поле	-
7		Категория контролируемого ресурса	УО	Если является объектом КИИ	[Без категории значимости] [Третья категория значимости] [Вторая категория значимости] [Первая категория значимости]	-
8		Код уровня атакуемого объекта/субъекта	О	-	Из классификатора «Типы объектов и субъектов», приведенного в приложении 28	-
9		Код типа атакуемого объекта/субъекта	О	-	Перечень зависит от поля «Код уровня атакуемого объекта/субъекта». Из классификатора «Типы объектов и субъектов», приведенного в приложении 28	Перечень зависит от поля «Код уровня атакуемого объекта/субъекта»
10		Наличие подключения к сети Интернет	О	-	[Да]	Предзаполненное поле
11		Страна/регион	О	-	В формате ISO-3166-2	-
12		IPv4-адрес атакованного ресурса	УО	Обязательно заполнение одного из полей	Список IP-адресов	-
13		IPv6-адрес атакованного ресурса				
14		Доменное имя атакованного ресурса			Список доменных имен	
15		URI-адрес атакованного ресурса			Список URI-адресов	
16		Атакованная сетевая служба и порт/протокол	УО	При наличии соответствующей информации	Текстовое поле	-
17	Сведения об объектах вредоносной активности, вызвавших компьютерный инцидент	Тип атаки	О	-	[DoS – Flood] [DoS- Vuln] [DDos]	-
18		Уровень OSI	О	-	[L2/3] [L3] [L4] [L6] [L7]	[L2/3] – канальный/сетевой уровень [L3] – сетевой уровень [L4] – транспортный уровень [L6] – уровень представления данных [L7] – прикладной уровень
19		IPv4-адрес вредоносного объекта	УО	Выявлен IPv4-адрес вредоносного объекта	Список IP-адресов или csv-файл	Заполняется хотя бы одно поле
20		IPv6-адрес вредоносного объекта		Выявлен IPv6-адрес вредоносного объекта		
21		Доменное имя вредоносного объекта	УО	Выявлено доменное имя вредоносного объекта	Список доменных имен или csv-файл	

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
22		Страна расположения вредоносного объекта	Н	-	Список трехбуквенных кодов стран в соответствии с ISO 3166	-
23		PPS (пакетов в секунду)	УО	Заполняется хотя бы одно поле	Вещественное число	-
24		Мб/с (мегабит в секунду)			Вещественное число	-
25		RPS (запросов в секунду)			Вещественное число	-
26		FPS (кадров в секунду)			Вещественное число	-
27		Перечень используемых уязвимостей	УО	Выявлен факт использования уязвимостей	-	Перечень используемых уязвимостей программного или аппаратного обеспечения в выбранной системе описания уязвимостей безопасности (например, CVE, БДУ ФСТЭК)
28		Наименование системы описания уязвимостей безопасности			Текстовое поле	
29	Оценка последствий компьютерного инцидента	Влияние на конфиденциальность	УО	При наличии указанных последствий	[Высокое] [Низкое]	-
30		Влияние на целостность			[Высокое] [Низкое]	-
31		Влияние на доступность			[Высокое] [Низкое]	-
32	Предпринятые меры по реагированию на компьютерный инцидент	Описание предпринятых действий в ходе реагирования на компьютерный инцидент	Н	-	Текстовое поле	-
33	Связь с другими уведомлениями	Вид связанного уведомления	УО	Заполняется в случае направления ранее в Банк России уведомления, связанного с текущим	[NTF_OWC] [NTF_ISI] [NTF_ORI] [NTF_CI] [NTF_CA] [NTF_VLN]	[NTF_OWC] – уведомление о выявленных случаях и (или) попытках осуществления переводов денежных средств без согласия клиента, а также о выявленных случаях и (или) попытках осуществления операций, направленных на совершение финансовых сделок с использованием финансовой платформы без волеизъявления участника финансовой платформы [NTF_ISI] – уведомление о выявлении инцидента защиты информации или результатах расследования инцидента защиты информации [NTF_ORI] – уведомление о выявлении инцидента операционной надежности или о результатах расследования инцидента операционной надежности [NTF_CI] – уведомление о компьютерных инцидентах [NTF_CA] – уведомления о компьютерных атаках [NTF_VLN] – уведомление о выявленных уязвимостях

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
34		Тип связи с другими уведомлениями			[Предшествующее событие] [Дочернее событие] [Связанное событие] [Уточнение сведений о событии]	-
35		Регистрационный номер уведомления			В соответствии с форматом АСОИ ФинЦЕРТ	Идентификатор уведомления или ответа на запрос, ранее направленного в ФинЦЕРТ участником информационного обмена
36	Ограничительный маркер TLP	Ограничительный маркер на распространение сведений из данного уведомления	Н	-	[TLP: WHITE] [TLP: GREEN] [TLP: AMBER] [TLP: RED]	В соответствии с обозначениями, принятыми в протоколе TLP. По умолчанию [TLP: GREEN], если не указано иное
37	Необходимость привлечения ФинЦЕРТ	Необходимость привлечения ФинЦЕРТ для устранения последствий компьютерного инцидента	УО	При необходимости	[Да]	-

Форма представления данных NTF_CI_Application compromise – Форма представления данных о компьютерном инциденте, связанном с успешной эксплуатацей уязвимости

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип уведомления	Тип уведомления	О	-	[NTF_CI_Application compromise]	Предзаполненное поле
2	Описание компьютерного инцидента	Описание компьютерного инцидента	Н	-	Текстовое поле	Текстовое описание компьютерного инцидента (в том числе дополнительные сведения о способе реализации КИ, способе выявления КИ и т. д.). В случае если компьютерный инцидент был выявлен с использованием сведений бюллетеня Банка России или НКЦКИ, необходимо указать номер данного бюллетеня
3	Классификация компьютерного инцидента	Вектор	О	-	[INT]	Предзаполненное поле
4		Тип компьютерного инцидента	О	-	[Application compromise]	Предзаполненное поле
5	Дата и время обнаружения	Дата и время выявления компьютерного инцидента	О	-	В соответствии с RFC 3339	По московскому времени [UTC +03:00]
6	Сведения об объектах, на которые направлен компьютерный инцидент	Наименование контролируемого информационного ресурса	О	-	Текстовое поле	-
7		Категория контролируемого ресурса	УО	Если является объектом КИИ	[Без категории значимости] [Третья категория значимости] [Вторая категория значимости] [Первая категория значимости]	-

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
8		Код уровня атакуемого объекта/субъекта	О	-	Из классификатора «Типы объектов и субъектов», приведенного в приложении 28	-
9		Код типа атакуемого объекта/субъекта	О	-	Перечень зависит от поля «Код уровня атакуемого объекта/субъекта». Из классификатора «Типы объектов и субъектов», приведенного в приложении 28	Перечень зависит от поля «Код уровня атакуемого объекта/субъекта»
10		Наличие подключения к сети Интернет	О	-	[Да]/[Нет]	-
11		Страна/регион	О	-	В формате ISO-3166-2	-
12		IPv4-адрес атакованного ресурса	УО	Обязательно заполнение одного из полей	Список IP-адресов	-
13		IPv6-адрес атакованного ресурса				
14		Доменное имя атакованного ресурса			Список доменных имен	
15		URI-адрес атакованного ресурса			Список URI-адресов	
16		Атакованная сетевая служба и порт/протокол	УО	При наличии соответствующей информации	Текстовое поле	-
17	Сведения об объектах вредоносной активности, вызвавших компьютерный инцидент	IPv4-адрес вредоносного объекта	УО	Выявлен IPv4-адрес вредоносного объекта	Список IP-адресов	-
18		IPv6-адрес вредоносного объекта		Выявлен IPv6-адрес вредоносного объекта		-
19		Доменное имя вредоносного объекта		Выявлено доменное имя вредоносного объекта	Список доменных имен	-
20		URI-адрес вредоносного объекта		Выявлен URI-адрес вредоносного объекта	Список URI-адресов	-
21		e-mail-адрес вредоносного объекта или субъекта		Выявлен e-mail-адрес вредоносного объекта или субъекта	Список e-mail-адресов	-
22		Уязвимость	УО	В случае если выявленная уязвимость описана в какой-либо системе описания уязвимостей	Перечень эксплуатируемых уязвимостей безопасности программного или аппаратного обеспечения, из соответствующего каталога (например, CVE, БДУ ФСТЭК и т. д.)	Обязательно заполняется один из блоков
23		Наименование системы описания уязвимостей			Текстовое поле	
24		Описание уязвимости	УО	В случае если выявленная уязвимость не описана ни в одной системе описания уязвимостей	Текстовое поле	

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
25		Описание объекта информатизации, в котором была проэксплуатирована уязвимость	О	-	В формате, соответствующем рекомендациям Банка России, опубликованными на официальном сайте	-
26	Сведения о незаконном раскрытии ПДн	Предполагаемые причины, повлекшие нарушение прав субъектов ПДн	УО	Блок заполняется в случае, если в результате компьютерного инцидента произошла утечка ПДн	Текстовое поле	Описание событий, которые привели к незаконному раскрытию информации. Поле заполняется, если в поле «Описание компьютерного инцидента» недостаточно информации о незаконном раскрытии ПДн
27		Характеристики ПДн			Текстовое поле	Указывается информация характеризующая незаконно раскрытые ПДн, в том числе тип субъекта, чьи ПДн были раскрыты, состав незаконно раскрытых ПДн, количество и актуальность записей и т. д.
28		Предполагаемый вред, нанесенный правам субъектов ПДн			Текстовое поле	Описание потенциального вреда, который может быть нанесен субъектам при использовании незаконно раскрытой информации
29		ФИО лица, уполномоченного оператором на взаимодействие с Роскомнадзором по инциденту			Текстовое поле	-
30		Мобильный телефон лица, уполномоченного на взаимодействие с Роскомнадзором по инциденту			В соответствии с российской системой и планом нумерации	-
31		Адрес электронной почты для отправки информации об уведомлении			В формате e-mail-адреса	-
32	Оценка последствий компьютерного инцидента	Влияние на конфиденциальность	УО	При наличии указанных последствий	[Высокое] [Низкое]	-
33		Влияние на целостность			[Высокое] [Низкое]	-
34		Влияние на доступность			[Высокое] [Низкое]	-
35	Предпринятые меры по реагированию на компьютерный инцидент	Описание предпринятых действий в ходе реагирования на компьютерный инцидент	Н	-	Текстовое поле	-

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
36	Связь с другими уведомлениями	Вид связанного уведомления	УО	Заполняется в случае направления ранее в Банк России уведомления, связанного с текущим	[NTF_OWC] [NTF_ISI] [NTF_ORI] [NTF_CI] [NTF_CA] [NTF_VLN]	[NTF_OWC] – уведомление о выявленных случаях и (или) попытках осуществления переводов денежных средств без согласия клиента, а также о выявленных случаях и (или) попытках осуществления операций, направленных на совершение финансовых сделок с использованием финансовой платформы без волеизъявления участника финансовой платформы [NTF_ISI] – уведомление о выявлении инцидента защиты информации или результатах расследования инцидента защиты информации [NTF_ORI] – уведомление о выявлении инцидента операционной надежности или о результатах расследования инцидента операционной надежности [NTF_CI] – уведомление о компьютерных инцидентах [NTF_CA] – уведомления о компьютерных атаках [NTF_VLN] – уведомление о выявленных уязвимостях
37		Тип связи с другими уведомлениями			[Предшествующее событие] [Дочернее событие] [Связанное событие] [Уточнение сведений о событии]	-
38		Регистрационный номер уведомления			В соответствии с форматом АСОИ ФинЦЕРТ	Идентификатор уведомления или ответа на запрос, ранее направленного в ФинЦЕРТ участником информационного обмена
39	Ограничительный маркер TLP	Ограничительный маркер на распространение сведений из данного уведомления	Н	-	[TLP: WHITE] [TLP: GREEN] [TLP: AMBER] [TLP: RED]	В соответствии с обозначениями, принятыми в протоколе TLP По умолчанию [TLP: GREEN], если не указано иное
40	Необходимость привлечения ФинЦЕРТ	Необходимость привлечения ФинЦЕРТ для устранения последствий компьютерного инцидента	УО	При необходимости	[Да]	-

Форма представления данных NTF_CI_Malware infection – Форма представления данных о компьютерном инциденте, связанном с заражением ВПО

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип уведомления	Тип уведомления	О	-	[NTF_CI_Malware infection]	Предзаполненное поле

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
2	Описание компьютерного инцидента	Описание компьютерного инцидента	Н	-	Текстовое поле	Текстовое описание компьютерного инцидента (в том числе дополнительные сведения о способе реализации КИ, способе выявления КИ и т. д.). В случае если компьютерный инцидент был выявлен с использованием сведений бюллетеня Банка России или НКЦКИ, необходимо указать номер данного бюллетеня
3	Классификация компьютерного инцидента	Вектор	О	-	[EXT] [INT]	[EXT] – направлено на клиента или контрагента финансовой организации или иных взаимодействующих с финансовой организации лиц [INT] – направлено на объекты информатизации финансовой организации
4		Тип компьютерного инцидента	О	-	[Malware infection]	Предзаполненное поле
5	Дата и время обнаружения	Дата и время выявления компьютерного инцидента	О	-	В соответствии с RFC 3339	По московскому времени [UTC +03:00]
6	Сведения об объектах, на которые направлен компьютерный инцидент	Наименование контролируемого информационного ресурса	О	-	Текстовое поле	-
7		Категория контролируемого ресурса	УО	Если является объектом КИИ	[Без категории значимости] [Третья категория значимости] [Вторая категория значимости] [Первая категория значимости]	-
8		Код уровня атакуемого объекта/субъекта	О	-	Из классификатора «Типы объектов и субъектов», приведенного в приложении 28	-
9		Код типа атакуемого объекта/субъекта	О	-	Перечень зависит от поля «Код уровня атакуемого объекта/субъекта». Из классификатора «Типы объектов и субъектов», приведенного в приложении 28	Перечень зависит от поля «Код уровня атакуемого объекта/субъекта»
10		Наличие подключения к сети Интернет	О	-	[Да]/[Нет]	-
11		Страна/регион	О	-	В формате ISO-3166-2	-
12		IPv4-адрес атакованного ресурса	УО	Обязательно заполнение одного из полей	Список IP-адресов	-
13		IPv6-адрес атакованного ресурса				
14		Доменное имя атакованного ресурса			Список доменных имен	
15		URI-адрес атакованного ресурса			Список URI-адресов	
16		e-mail-адрес атакованного объекта			Список e-mail-адресов	

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
17		Атакованная сетевая служба и порт/протокол	УО	При наличии соответствующей информации	Текстовое поле	-
18	Сведения об объектах вредоносной активности, вызвавших компьютерный инцидент	IPv4-адрес вредоносного объекта	УО	Выявлен IPv4-адрес вредоносного объекта	Список IP-адресов	-
19		IPv6-адрес вредоносного объекта		Выявлен IPv6-адрес вредоносного объекта		-
20		Доменное имя вредоносного объекта		Выявлено доменное имя вредоносного объекта	Список доменных имен	-
21		URI-адрес вредоносного объекта		Выявлен URI-адрес вредоносного объекта	Список URI-адресов	-
22		e-mail-адрес вредоносного объекта или субъекта		Выявлен e-mail-адрес вредоносного объекта или субъекта	Список e-mail-адресов	-
23		Название антивируса, выявившего заражение ВПО	УО	Если ВПО было выявлено антивирусом	Текстовое поле	-
24		Описание и классификация вредоносного ПО	Н	-	Текстовое поле	-
25		Сетевая активность	УО	При наличии информации о сетевой активности ВПО	Текстовое поле	-
26		Уязвимость	УО	В случае если выявлен факт эксплуатации уязвимостей ВПО	Перечень эксплуатируемых уязвимостей безопасности программного или аппаратного обеспечения, из соответствующего каталога (например, CVE, БДУ ФСТЭК и т. д.)	-
27		Наименование системы описания уязвимостей			Текстовое поле	-
28		Описание уязвимости, не описанной ни в одной системе описания уязвимостей			Текстовое поле	-
29		Файл ВПО	УО	Обязательно заполняется одно из полей	Файл	-
30		URL для скачивания			Текстовое поле	-
31		Хеш-сумма	О	-	Текстовое поле	-
32		Алгоритм хеширования		-	[SHA256] [SHA1] [MD5]	-
33	Сведения о незаконном раскрытии ПДн	Предполагаемые причины, повлекшие нарушение прав субъектов ПДн	УО	Блок заполняется в случае, если в результате компьютерного инцидента произошла утечка ПДн	Текстовое поле	Описание событий, которые привели к незаконному раскрытию информации. Поле заполняется, если в поле «Описание компьютерного инцидента» недостаточно информации о незаконном раскрытии ПДн

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
34		Характеристики ПДн			Текстовое поле	Указывается информация характеризующая незаконно раскрытые ПДн, в том числе тип субъекта, чьи ПДн были раскрыты, состав незаконно раскрытых ПДн, количество и актуальность записей и т. д.
35		Предполагаемый вред, нанесенный правам субъектов ПДн			Текстовое поле	Описание потенциального вреда, который может быть нанесен субъектам при использовании незаконно раскрытой информации
36		ФИО лица, уполномоченного оператором на взаимодействие с Роскомнадзором по инциденту			Текстовое поле	-
37		Мобильный телефон лица, уполномоченного на взаимодействие с Роскомнадзором по инциденту			В соответствии с российской системой и планом нумерации	-
38		Адрес электронной почты для отправки информации об уведомлении			В формате e-mail-адреса	-
39	Оценка последствий компьютерного инцидента	Влияние на конфиденциальность	УО	При наличии указанных последствий	[Высокое] [Низкое]	-
40		Влияние на целостность			[Высокое] [Низкое]	-
41		Влияние на доступность			[Высокое] [Низкое]	-
42	Предпринятые меры по реагированию на компьютерный инцидент	Описание предпринятых действий в ходе реагирования на компьютерный инцидент	Н	-	Текстовое поле	-

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
43	Связь с другими уведомлениями	Вид связанного уведомления	УО	Заполняется в случае направления ранее в Банк России уведомления, связанного с текущим	[NTF_OWC] [NTF_ISI] [NTF_ORI] [NTF_CI] [NTF_CA] [NTF_VLN]	[NTF_OWC] – уведомление о выявленных случаях и (или) попытках осуществления переводов денежных средств без согласия клиента, а также о выявленных случаях и (или) попытках осуществления операций, направленных на совершение финансовых сделок с использованием финансовой платформы без волеизъявления участника финансовой платформы [NTF_ISI] – уведомление о выявлении инцидента защиты информации или результатах расследования инцидента защиты информации [NTF_ORI] – уведомление о выявлении инцидента операционной надежности или о результатах расследования инцидента операционной надежности [NTF_CI] – уведомление о компьютерных инцидентах [NTF_CA] – уведомления о компьютерных атаках [NTF_VLN] – уведомление о выявленных уязвимостях
44		Тип связи с другими уведомлениями			[Предшествующее событие] [Дочернее событие] [Связанное событие] [Уточнение сведений о событии]	-
45		Регистрационный номер уведомления			В соответствии с форматом АСОИ ФинЦЕРТ	Идентификатор уведомления или ответа на запрос, ранее направленного в ФинЦЕРТ участником информационного обмена
46	Ограничительный маркер TLP	Ограничительный маркер на распространение сведений из данного уведомления	Н	-	[TLP: WHITE] [TLP: GREEN] [TLP: AMBER] [TLP: RED]	В соответствии с обозначениями, принятыми в протоколе TLP. По умолчанию [TLP: GREEN], если не указано иное
47	Необходимость привлечения ФинЦЕРТ	Необходимость привлечения ФинЦЕРТ для устранения последствий компьютерного инцидента	УО	При необходимости	[Да]	-

Форма представления данных NTF_CI_Account compromise – Форма представления данных о компьютерном инциденте, связанном с компрометацией учетной записи

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип уведомления	Тип уведомления	О	-	[NTF_CI_Account compromise]	Предзаполненное поле

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
2	Описание компьютерного инцидента	Описание компьютерного инцидента	Н	-	Текстовое поле	Текстовое описание компьютерного инцидента (в том числе дополнительные сведения о способе реализации КИ, способе выявления КИ и т. д.). В случае если компьютерный инцидент был выявлен с использованием сведений бюллетеня Банка России или НКЦКИ, необходимо указать номер данного бюллетеня
3	Классификация компьютерного инцидента	Вектор	О	-	[EXT] [INT]	[EXT] – направлено на клиента или контрагента финансовой организации или иных взаимодействующих с финансовой организации лиц [INT] – направлено на объекты информатизации финансовой организации
4		Тип компьютерного инцидента	О	-	[Account compromise]	Предзаполненное поле
5	Дата и время обнаружения	Дата и время выявления компьютерного инцидента	О	-	В соответствии с RFC 3339	По московскому времени [UTC +03:00]
6	Сведения об объектах, на которые направлен компьютерный инцидент	Наименование контролируемого информационного ресурса	О	-	Текстовое поле	-
7		Категория контролируемого ресурса	УО	Если является объектом КИИ	[Без категории значимости] [Третья категория значимости] [Вторая категория значимости] [Первая категория значимости]	-
8		Код уровня атакуемого объекта/субъекта	О	-	Из классификатора «Типы объектов и субъектов», приведенного в приложении 28	-
9		Код типа атакуемого объекта/субъекта	О	-	Перечень зависит от поля «Код уровня атакуемого объекта/субъекта». Из классификатора «Типы объектов и субъектов» , приведенного в приложении 28	Перечень зависит от поля «Код уровня атакуемого объекта/субъекта»
10		Наличие подключения к сети Интернет	О	-	[Да]/[Нет]	-
11		Страна/регион	О	-	В формате ISO-3166-2	-
12		IPv4-адрес атакованного ресурса	УО	Обязательно заполнение одного из полей	Список IP-адресов	-
13		IPv6-адрес атакованного ресурса				
14		Доменное имя атакованного ресурса			Список доменных имен	
15		URI-адрес атакованного ресурса			Список URI-адресов	
16		e-mail-адрес атакованного объекта			Список e-mail-адресов	

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
17		Атакованная сетевая служба и порт/протокол	УО	При наличии соответствующей информации	Текстовое поле	-
18	Сведения об объектах вредоносной активности, вызвавших компьютерный инцидент	IPv4-адрес вредоносного объекта	УО	Выявлен IPv4-адрес вредоносного объекта	Список IP-адресов	-
19		IPv6-адрес вредоносного объекта		Выявлен IPv6-адрес вредоносного объекта		-
20		Доменное имя вредоносного объекта		Выявлено доменное имя вредоносного объекта	Список доменных имен	-
21		Логин скомпрометированной УЗ	О	-	Текстовое поле	-
22		Привилегии скомпрометированной УЗ	О	-	Текстовое поле	-
23		Способ компрометации	УО	При наличии соответствующей информации	Текстовое поле	-
24	Сведения о незаконном раскрытии ПДн	Предполагаемые причины, повлекшие нарушение прав субъектов ПДн	УО	Блок заполняется в случае, если в результате компьютерного инцидента произошла утечка ПДн	Текстовое поле	Описание событий, которые привели к незаконному раскрытию информации. Поле заполняется, если в поле «Описание компьютерного инцидента» недостаточно информации о незаконном раскрытии ПДн
25		Характеристики ПДн			Текстовое поле	Указывается информация характеризующая незаконно раскрытые ПДн, в том числе тип субъекта, чьи ПДн были раскрыты, состав незаконно раскрытых ПДн, количество и актуальность записей и т. д.
26		Предполагаемый вред, нанесенный правам субъектов ПДн			Текстовое поле	Описание потенциального вреда, который может быть нанесен субъектам при использовании незаконно раскрытой информации
27		ФИО лица, уполномоченного оператором на взаимодействие с Роскомнадзором по инциденту			Текстовое поле	-
28		Мобильный телефон лица, уполномоченного на взаимодействие с Роскомнадзором по инциденту			В соответствии с российской системой и планом нумерации	-
29		Адрес электронной почты для отправки информации об уведомлении			В формате e-mail-адреса	-
30	Оценка последствий компьютерного инцидента	Влияние на конфиденциальность	УО	При наличии указанных последствий	[Высокое] [Низкое]	-
31		Влияние на целостность			[Высокое] [Низкое]	-
32		Влияние на доступность			[Высокое] [Низкое]	-

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
33	Предпринятые меры по реагированию на компьютерный инцидент	Описание предпринятых действий в ходе реагирования на компьютерный инцидент	Н	-	Текстовое поле	-
34	Связь с другими уведомлениями	Вид связанного уведомления	УО	Заполняется в случае направления ранее в Банк России уведомления, связанного с текущим	[NTF_OWC] [NTF_ISI] [NTF_ORI] [NTF_CI] [NTF_CA] [NTF_VLN]	[NTF_OWC] – уведомление о выявленных случаях и (или) попытках осуществления переводов денежных средств без согласия клиента, а также о выявленных случаях и (или) попытках осуществления операций, направленных на совершение финансовых сделок с использованием финансовой платформы без волеизъявления участника финансовой платформы [NTF_ISI] – уведомление о выявлении инцидента защиты информации или результатах расследования инцидента защиты информации [NTF_ORI] – уведомление о выявлении инцидента операционной надежности или о результатах расследования инцидента операционной надежности [NTF_CI] – уведомление о компьютерных инцидентах [NTF_CA] – уведомления о компьютерных атаках [NTF_VLN] – уведомление о выявленных уязвимостях
35		Тип связи с другими уведомлениями			[Предшествующее событие] [Дочернее событие] [Связанное событие] [Уточнение сведений о событии]	-
36		Регистрационный номер уведомления			В соответствии с форматом АСОИ ФинЦЕРТ	Идентификатор уведомления или ответа на запрос, ранее направленного в ФинЦЕРТ участником информационного обмена
37	Ограничительный маркер TLP	Ограничительный маркер на распространение сведений из данного уведомления	Н	-	[TLP: WHITE] [TLP: GREEN] [TLP: AMBER] [TLP: RED]	В соответствии с обозначениями, принятыми в протоколе TLP. По умолчанию [TLP: GREEN], если не указано иное
38	Необходимость привлечения ФинЦЕРТ	Необходимость привлечения ФинЦЕРТ для устранения последствий компьютерного инцидента	УО	При необходимости	[Да]	-

Форма представления данных NTF_CI_Prohibited content – Форма представления данных о компьютерном инциденте, связанном с публикацией на контролируемом ресурсе запрещенной законодательством РФ информации

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип уведомления	Тип уведомления	О	-	[NTF_CI_Prohibited content]	Предзаполненное поле

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
2	Описание компьютерного инцидента	Описание компьютерного инцидента	Н	-	Текстовое поле	Текстовое описание компьютерного инцидента (в том числе дополнительные сведения о способе реализации КИ, способе выявления КИ и т. д.). В случае если компьютерный инцидент был выявлен с использованием сведений бюллетеня Банка России или НКЦКИ, необходимо указать номер данного бюллетеня
3	Классификация компьютерного инцидента	Вектор	О	-	[INT]	Предзаполненное поле
4		Тип компьютерного инцидента	О	-	[Prohibited content]	Предзаполненное поле
5	Дата и время обнаружения	Дата и время выявления компьютерного инцидента	О	-	В соответствии с RFC 3339	По московскому времени [UTC +03:00]
6	Сведения об объектах, на которые направлен компьютерный инцидент	Наименование контролируемого информационного ресурса	О	-	Текстовое поле	-
7		Категория контролируемого ресурса	УО	Если является объектом КИИ	[Без категории значимости] [Третья категория значимости] [Вторая категория значимости] [Первая категория значимости]	-
8		Код уровня атакуемого объекта/субъекта	О	-	Из классификатора «Типы объектов и субъектов», приведенного в приложении 28	-
9		Код типа атакуемого объекта/субъекта	О	-	Перечень зависит от поля «Код уровня атакуемого объекта/субъекта». Из классификатора «Типы объектов и субъектов», приведенного в приложении 28	Перечень зависит от поля «Код уровня атакуемого объекта/субъекта»
10		Наличие подключения к сети Интернет	О	-	[Да]/[Нет]	-
11		Страна/регион	О	-	В формате ISO-3166-2	-
12		IPv4-адрес атакованного ресурса	УО	Обязательно заполнение одного из полей	Список IP-адресов	-
13		IPv6-адрес атакованного ресурса				
14		Доменное имя атакованного ресурса			Список доменных имен	
15		URI-адрес атакованного ресурса			Список URI-адресов	
16	Сведения об объектах вредоносной активности, вызвавших компьютерный инцидент	IPv4-адрес вредоносного объекта	УО	Выявлен IPv4-адрес вредоносного объекта	Список IP-адресов	-

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
17		IPv6-адрес вредоносного объекта		Выявлен IPv6-адрес вредоносного объекта		-
18		Доменное имя вредоносного объекта		Выявлено доменное имя вредоносного объекта	Список доменных имен	-
19		URI-адрес вредоносного объекта		Выявлен URI-адрес вредоносного объекта	Список URI-адресов	-
20	Оценка последствий компьютерного инцидента	Влияние на конфиденциальность	УО	При наличии указанных последствий	[Высокое] [Низкое]	-
21		Влияние на целостность			[Высокое] [Низкое]	-
22		Влияние на доступность			[Высокое] [Низкое]	-
23	Предпринятые меры по реагированию на компьютерный инцидент	Описание предпринятых действий в ходе реагирования на компьютерный инцидент	Н	-	Текстовое поле	-
24	Связь с другими уведомлениями	Вид связанного уведомления	УО	Заполняется в случае направления ранее в Банк России уведомления, связанного с текущим	[NTF_OWC] [NTF_ISI] [NTF_ORI] [NTF_CI] [NTF_CA] [NTF_VLN]	[NTF_OWC] – уведомление о выявленных случаях и (или) попытках осуществления переводов денежных средств без согласия клиента, а также о выявленных случаях и (или) попытках осуществления операций, направленных на совершение финансовых сделок с использованием финансовой платформы без волеизъявления участника финансовой платформы [NTF_ISI] – уведомление о выявлении инцидента защиты информации или результатах расследования инцидента защиты информации [NTF_ORI] – уведомление о выявлении инцидента операционной надежности или о результатах расследования инцидента операционной надежности [NTF_CI] – уведомление о компьютерных инцидентах [NTF_CA] – уведомления о компьютерных атаках [NTF_VLN] – уведомление о выявленных уязвимостях
25		Тип связи с другими уведомлениями			[Предшествующее событие] [Дочернее событие] [Связанное событие] [Уточнение сведений о событии]	-
26		Регистрационный номер уведомления			В соответствии с форматом АСОИ ФинЦЕРТ	Идентификатор уведомления или ответа на запрос, ранее направленного в ФинЦЕРТ участником информационного обмена

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
27	Ограничительный маркер TLP	Ограничительный маркер на распространение сведений из данного уведомления	Н	-	[TLP: WHITE] [TLP: GREEN] [TLP: AMBER] [TLP: RED]	В соответствии с обозначениями, принятыми в протоколе TLP По умолчанию [TLP: GREEN], если не указано иное
28	Необходимость привлечения ФинЦЕРТ	Необходимость привлечения ФинЦЕРТ для устранения последствий компьютерного инцидента	УО	При необходимости	[Да]	-

Форма представления данных NTF_CI_Social engineering – Форма представления данных о компьютерном инциденте, связанном с Социальной инженерей

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип уведомления	Тип уведомления	О	-	[NTF_CI_Social engineering]	Предзаполненное поле
2	Описание компьютерного инцидента	Описание компьютерного инцидента	Н	-	Текстовое поле	Текстовое описание компьютерного инцидента (в том числе дополнительные сведения о способе реализации КИ, способе выявления КИ и т. д.). В случае если компьютерный инцидент был выявлен с использованием сведений бюллетеня Банка России или НКЦКИ, необходимо указать номер данного бюллетеня
3	Классификация компьютерного инцидента	Вектор	О	-	[EXT] [INT]	[EXT] – направлено на клиента или контрагента финансовой организации или иных взаимодействующих с финансовой организации лиц [INT] – направлено на объекты информатизации финансовой организации
4		Тип компьютерного инцидента	О	-	[Social engineering]	Предзаполненное поле
5	Дата и время обнаружения	Дата и время выявления компьютерного инцидента	О	-	В соответствии с RFC 3339	По московскому времени [UTC +03:00]
6	Сведения об объектах, на которые направлен компьютерный инцидент	Код уровня атакуемого объекта/субъекта	О	-	[Subject]	Предзаполненное поле
7		Код типа атакуемого объекта/субъекта	О	-	Из классификатора «Типы объектов и субъектов», приведенного в приложении 28 [Employee] [Client] [Partner]	-
8	Сведения об объектах вредоносной активности, вызвавших компьютерный инцидент	IPv4-адрес вредоносного объекта	УО	Выявлен IPv4-адрес вредоносного объекта	Список IP-адресов	Заполняется хотя бы одно поле

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
9		IPv6-адрес вредоносного объекта		Выявлен IPv6-адрес вредоносного объекта		
10		Доменное имя вредоносного объекта		Выявлено доменное имя вредоносного объекта	Список доменных имен	
11		URI-адрес вредоносного объекта		Выявлен URI-адрес вредоносного объекта	Список URI-адресов	
12		e-mail-адрес вредоносного объекта или субъекта		Выявлен e-mail-адрес вредоносного объекта или субъекта	Список e-mail-адресов	
13		Абонентский номер подвижной радиотелефонной связивредоносного субъекта		Выявлен абонентский номер подвижной радиотелефонной связи вредоносного субъекта	Список номеров в соответствии с российской системой и планом нумерации	
14		Канал взаимодействия	О	-	[Телефонный звонок] [СМС] [Электронная почта] [Система обмена мгновенными сообщениями] [Сайт] [Иной канал]	-
15		Текст сообщения	УО	«Канал взаимодействия» = { [СМС], [Электронная почта], [Система обмена мгновенными сообщениями]}	Тестовое поле или txt-файл	-
16	Оценка последствий компьютерного инцидента	Влияние на конфиденциальность	УО	При наличии указанных последствий	[Высокое] [Низкое]	-
17		Влияние на целостность			[Высокое] [Низкое]	-
18		Влияние на доступность			[Высокое] [Низкое]	-
19	Предпринятые меры по реагированию на компьютерный инцидент	Описание предпринятых действий в ходе реагирования на компьютерный инцидент	Н	-	Текстовое поле	-

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
20	Связь с другими уведомлениями	Вид связанного уведомления	УО	Заполняется в случае направления ранее в Банк России уведомления, связанного с текущим	[NTF_OWC] [NTF_ISI] [NTF_ORI] [NTF_CI] [NTF_CA] [NTF_VLN]	[NTF_OWC] – уведомление о выявленных случаях и (или) попытках осуществления переводов денежных средств без согласия клиента, а также о выявленных случаях и (или) попытках осуществления операций, направленных на совершение финансовых сделок с использованием финансовой платформы без волеизъявления участника финансовой платформы [NTF_ISI] – уведомление о выявлении инцидента защиты информации или результатах расследования инцидента защиты информации [NTF_ORI] – уведомление о выявлении инцидента операционной надежности или о результатах расследования инцидента операционной надежности [NTF_CI] – уведомление о компьютерных инцидентах [NTF_CA] – уведомления о компьютерных атаках [NTF_VLN] – уведомление о выявленных уязвимостях
21		Тип связи с другими уведомлениями			[Предшествующее событие] [Дочернее событие] [Связанное событие] [Уточнение сведений о событии]	-
22		Регистрационный номер уведомления			В соответствии с форматом АСОИ ФинЦЕРТ	Идентификатор уведомления или ответа на запрос, ранее направленного в ФинЦЕРТ участником информационного обмена
23	Ограничительный маркер TLP	Ограничительный маркер на распространение сведений из данного уведомления	Н	-	[TLP: WHITE] [TLP: GREEN] [TLP: AMBER] [TLP: RED]	В соответствии с обозначениями, принятыми в протоколе TLP. По умолчанию [TLP: GREEN], если не указано иное
24	Необходимость привлечения ФинЦЕРТ	Необходимость привлечения ФинЦЕРТ для устранения последствий компьютерного инцидента	УО	При необходимости	[Да]	-

Форма представления данных NTF_CI_Traffic hijacking – Форма представления данных о компьютерном инциденте, связанном с захватом сетевого трафика

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип уведомления	Тип уведомления	О	-	[NTF_CI_Traffic hijacking]	Предзаполненное поле

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
2	Описание компьютерного инцидента	Описание компьютерного инцидента	Н	-	Текстовое поле	Текстовое описание компьютерного инцидента (в том числе дополнительные сведения о способе реализации КИ, способе выявления КИ и т. д.). В случае если компьютерный инцидент был выявлен с использованием сведений бюллетеня Банка России или НКЦКИ, необходимо указать номер данного бюллетеня
3	Классификация компьютерного инцидента	Вектор	О	-	[INT]	Предзаполненное поле
4		Тип компьютерного инцидента	О	-	[Traffic hijacking]	Предзаполненное поле
5	Дата и время обнаружения	Дата и время выявления компьютерного инцидента	О	-	В соответствии с RFC 3339	По московскому времени [UTC +03:00]
6	Сведения об объектах, на которые направлен компьютерный инцидент	Наименование контролируемого информационного ресурса	О	-	Текстовое поле	-
7		Категория контролируемого ресурса	УО	Если является объектом КИИ	[Без категории значимости] [Третья категория значимости] [Вторая категория значимости] [Первая категория значимости]	-
8		Код уровня атакуемого объекта/субъекта	О	-	Из классификатора «Типы объектов и субъектов», приведенного в приложении 28	-
9		Код типа атакуемого объекта/субъекта	О	-	Перечень зависит от поля «Код уровня атакуемого объекта/субъекта». Из классификатора «Типы объектов и субъектов», приведенного в приложении 28	Перечень зависит от поля «Код уровня атакуемого объекта/субъекта»
10		Наличие подключения к сети Интернет	О	-	[Да]/[Нет]	-
11		Страна/регион	О	-	В формате ISO-3166-2	-
12		AS-Path до атакованной автономной системы (ASN)			Текстовое поле	
13	Сведения об объектах вредоносной активности, вызвавших компьютерный инцидент	Номер подставной автономной системы (ASN)	О	-	Текстовое поле	-
14		Наименование AS	О	-	Текстовое поле	-
15		Наименование LIR	О	-	Текстовое поле	-
16		Ссылка на Looking Glass	УО	При наличии	Текстовое поле	-
17		Штатный prefix	Н	-	Текстовое поле	-
18		Подставной prefix	Н	-	Текстовое поле	-

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
19	Оценка последствий компьютерного инцидента	Влияние на конфиденциальность	УО	При наличии указанных последствий	[Высокое] [Низкое]	-
20		Влияние на целостность			[Высокое] [Низкое]	-
21		Влияние на доступность			[Высокое] [Низкое]	-
22	Предпринятые меры по реагированию на компьютерный инцидент	Описание предпринятых действий в ходе реагирования на компьютерный инцидент	Н	-	Текстовое поле	-
23	Связь с другими уведомлениями	Вид связанного уведомления	УО	Заполняется в случае направления ранее в Банк России уведомления, связанного с текущим	[NTF_OWC] [NTF_ISI] [NTF_ORI] [NTF_CI] [NTF_CA] [NTF_VLN]	[NTF_OWC] – уведомление о выявленных случаях и (или) попытках осуществления переводов денежных средств без согласия клиента, а также о выявленных случаях и (или) попытках осуществления операций, направленных на совершение финансовых сделок с использованием финансовой платформы без волеизъявления участника финансовой платформы [NTF_ISI] – уведомление о выявлении инцидента защиты информации или результатах расследования инцидента защиты информации [NTF_ORI] – уведомление о выявлении инцидента операционной надежности или о результатах расследования инцидента операционной надежности [NTF_CI] – уведомление о компьютерных инцидентах [NTF_CA] – уведомления о компьютерных атаках [NTF_VLN] – уведомление о выявленных уязвимостях
24		Тип связи с другими уведомлениями			[Предшествующее событие] [Дочернее событие] [Связанное событие] [Уточнение сведений о событии]	-
25		Регистрационный номер уведомления			В соответствии с форматом АСОИ ФинЦЕРТ	Идентификатор уведомления или ответа на запрос, ранее направленного в ФинЦЕРТ участником информационного обмена
26	Ограничительный маркер TLP	Ограничительный маркер на распространение сведений из данного уведомления	Н	-	[TLP: WHITE] [TLP: GREEN] [TLP: AMBER] [TLP: RED]	В соответствии с обозначениями, принятыми в протоколе TLP. По умолчанию [TLP: GREEN], если не указано иное
27	Необходимость привлечения ФинЦЕРТ	Необходимость привлечения ФинЦЕРТ для устранения последствий компьютерного инцидента	УО	При необходимости	[Да]	-

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание

Форма представления данных NTF_CI_Unauthorised modification – Форма представления данных о компьютерном инциденте, связанном с несанкционированным изменением информации

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип уведомления	Тип уведомления	О	-	[NTF_CI_Unauthorised modification]	Предзаполненное поле
2	Описание компьютерного инцидента	Описание компьютерного инцидента	Н	-	Текстовое поле	Текстовое описание компьютерного инцидента (в том числе дополнительные сведения о способе реализации КИ, способе выявления КИ и т. д.). В случае если компьютерный инцидент был выявлен с использованием сведений бюллетеня Банка России или НКЦКИ, необходимо указать номер данного бюллетеня
3	Классификация компьютерного инцидента	Вектор	О	-	[INT]	Предзаполненное поле
4		Тип компьютерного инцидента	О	-	[Unauthorised modification]	Предзаполненное поле
5	Дата и время обнаружения	Дата и время выявления компьютерного инцидента	О	-	В соответствии с RFC 3339	По московскому времени [UTC +03:00]
6	Сведения об объектах, на которые направлен компьютерный инцидент	Наименование контролируемого информационного ресурса	О	-	Текстовое поле	-
7		Категория контролируемого ресурса	УО	Если является объектом КИИ	[Без категории значимости] [Третья категория значимости] [Вторая категория значимости] [Первая категория значимости]	-
8		Код уровня атакуемого объекта/субъекта	О	-	Из классификатора «Типы объектов и субъектов», приведенного в приложении 28	-
9		Код типа атакуемого объекта/субъекта	О	-	Перечень зависит от поля «Код уровня атакуемого объекта/субъекта». Из классификатора «Типы объектов и субъектов», приведенного в приложении 28	Перечень зависит от поля «Код уровня атакуемого объекта/субъекта»
10		Наличие подключения к сети Интернет	О	-	[Да]/[Нет]	-
11		Страна/регион	О	-	В формате ISO-3166-2	-
12		IPv4-адрес атакованного ресурса	УО	Обязательно заполнение одного из полей	Список IP-адресов	-
13		IPv6-адрес атакованного ресурса				
14		Доменное имя атакованного ресурса			Список доменных имен	

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
15		URI-адрес атакованного ресурса			Список URI-адресов	
16		Атакованная сетевая служба и порт/протокол	УО	При наличии соответствующей информации	Текстовое поле	-
17	Сведения об объектах вредоносной активности, вызвавших компьютерный инцидент	IPv4-адрес вредоносного объекта	УО	Выявлен IPv4-адрес вредоносного объекта	Список IP-адресов	-
18		IPv6-адрес вредоносного объекта		Выявлен IPv6-адрес вредоносного объекта		-
19		Доменное имя вредоносного объекта		Выявлено доменное имя вредоносного объекта	Список доменных имен	-
20		URI-адрес вредоносного объекта		Выявлен URI-адрес вредоносного объекта	Список URI-адресов	-
21	Оценка последствий компьютерного инцидента	Влияние на конфиденциальность	УО	При наличии указанных последствий	[Высокое] [Низкое]	-
22		Влияние на целостность			[Высокое] [Низкое]	-
23		Влияние на доступность			[Высокое] [Низкое]	-
24	Предпринятые меры по реагированию на компьютерный инцидент	Описание предпринятых действий в ходе реагирования на компьютерный инцидент	Н	-	Текстовое поле	-
25	Связь с другими уведомлениями	Вид связанного уведомления	УО	Заполняется в случае направления ранее в Банк России уведомления, связанного с текущим	[NTF_OWC] [NTF_ISI] [NTF_ORI] [NTF_CI] [NTF_CA] [NTF_VLN]	[NTF_OWC] – уведомление о выявленных случаях и (или) попытках осуществления переводов денежных средств без согласия клиента, а также о выявленных случаях и (или) попытках осуществления операций, направленных на совершение финансовых сделок с использованием финансовой платформы без волеизъявления участника финансовой платформы [NTF_ISI] – уведомление о выявлении инцидента защиты информации или результатах расследования инцидента защиты информации [NTF_ORI] – уведомление о выявлении инцидента операционной надежности или о результатах расследования инцидента операционной надежности [NTF_CI] – уведомление о компьютерных инцидентах [NTF_CA] – уведомления о компьютерных атаках [NTF_VLN] – уведомление о выявленных уязвимостях

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
26		Тип связи с другими уведомлениями			[Предшествующее событие] [Дочернее событие] [Связанное событие] [Уточнение сведений о событии]	-
27		Регистрационный номер уведомления			В соответствии с форматом АСОИ ФинЦЕРТ	Идентификатор уведомления или ответа на запрос, ранее направленного в ФинЦЕРТ участником информационного обмена
28	Ограничительный маркер TLP	Ограничительный маркер на распространение сведений из данного уведомления	Н	-	[TLP: WHITE] [TLP: GREEN] [TLP: AMBER] [TLP: RED]	В соответствии с обозначениями, принятыми в протоколе TLP. По умолчанию [TLP: GREEN], если не указано иное
29	Необходимость привлечения ФинЦЕРТ	Необходимость привлечения ФинЦЕРТ для устранения последствий компьютерного инцидента	УО	При необходимости	[Да]	-

Форма представления данных NTF_CI_Unauthorised access – Форма представления данных о компьютерном инциденте, связанном с несанкционированным разглашением информации

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип уведомления	Тип уведомления	О	-	[NTF_CI_Unauthorised access]	Предзаполненное поле
2	Описание компьютерного инцидента	Описание компьютерного инцидента	Н	-	Текстовое поле	Текстовое описание компьютерного инцидента (в том числе дополнительные сведения о способе реализации КИ, способе выявления КИ и т. д.). В случае если компьютерный инцидент был выявлен с использованием сведений бюллетеня Банка России или НКЦКИ, необходимо указать номер данного бюллетеня
3	Классификация компьютерного инцидента	Вектор	О	-	[INT]	Предзаполненное поле
4		Тип компьютерного инцидента	О	-	[Unauthorised access]	Предзаполненное поле
5	Дата и время обнаружения	Дата и время выявления компьютерного инцидента	О	-	В соответствии с RFC 3339	По московскому времени [UTC +03:00]
6	Сведения об объектах, на которые направлен компьютерный инцидент	Наименование контролируемого информационного ресурса	О	-	Текстовое поле	-
7		Категория контролируемого ресурса	УО	Если является объектом КИИ	[Без категории значимости] [Третья категория значимости] [Вторая категория значимости] [Первая категория значимости]	-

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
8		Код уровня атакуемого объекта/субъекта	О	-	Из классификатора «Типы объектов и субъектов», приведенного в приложении 28	-
9		Код типа атакуемого объекта/субъекта	О	-	Перечень зависит от поля «Код уровня атакуемого объекта/субъекта». Из классификатора «Типы объектов и субъектов», приведенного в приложении 28	Перечень зависит от поля «Код уровня атакуемого объекта/субъекта»
10		Наличие подключения к сети Интернет	О	-	[Да]/[Нет]	-
11		Страна/регион	О	-	В формате ISO-3166-2	-
12		IPv4-адрес атакованного ресурса	УО	Обязательно заполнение одного из полей	Список IP-адресов	-
13		IPv6-адрес атакованного ресурса				
14		Доменное имя атакованного ресурса			Список доменных имен	
15		URI-адрес атакованного ресурса			Список URI-адресов	
16		e-mail-адрес атакованного объекта			Список e-mail-адресов	
17		Атакованная сетевая служба и порт/протокол	УО	При наличии соответствующей информации	Текстовое поле	-
18	Сведения об объектах вредоносной активности, вызвавших компьютерный инцидент	IPv4-адрес вредоносной системы	УО	Выявлен IPv4-адрес вредоносной системы или объекта	Список IP-адресов	-
19		IPv6-адрес вредоносной системы		Выявлен IPv6-адрес вредоносной системы или объекта		-
20		Доменное имя вредоносной системы		Выявлено доменное имя вредоносной системы или объекта	Список доменных имен	-
21		e-mail-адрес вредоносного объекта		Выявлен e-mail-адрес вредоносной системы или объекта	Список e-mail-адресов	-
22	Сведения о незаконном раскрытии ПДн	Предполагаемые причины, повлекшие нарушение прав субъектов ПДн	УО	Блок заполняется в случае, если в результате компьютерного инцидента произошла утечка ПДн	Текстовое поле	Описание событий, которые привели к незаконному раскрытию информации. Поле заполняется, если в поле «Описание компьютерного инцидента» недостаточно информации о незаконном раскрытии ПДн
23		Характеристики ПДн			Текстовое поле	Указывается информация характеризующая незаконно раскрытые ПДн, в том числе тип субъекта, чьи ПДн были раскрыты, состав незаконно раскрытых ПДн, количество и актуальность записей и т. д.

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
24		Предполагаемый вред, нанесенный правам субъектов ПДн			Текстовое поле	Описание потенциального вреда, который может быть нанесен субъектам при использовании незаконно раскрытой информации
25		ФИО лица, уполномоченного оператором на взаимодействие с Роскомнадзором по инциденту			Текстовое поле	-
26		Мобильный телефон лица, уполномоченного на взаимодействие с Роскомнадзором по инциденту			В соответствии с российской системой и планом нумерации	-
27		Адрес электронной почты для отправки информации об уведомлении			В формате e-mail-адреса	-
28	Оценка последствий компьютерного инцидента	Влияние на конфиденциальность	УО	При наличии указанных последствий	[Высокое] [Низкое]	-
29		Влияние на целостность			[Высокое] [Низкое]	-
30		Влияние на доступность			[Высокое] [Низкое]	-
31	Предпринятые меры по реагированию на компьютерный инцидент	Описание предпринятых действий в ходе реагирования на компьютерный инцидент	Н	-	Текстовое поле	-
32	Связь с другими уведомлениями	Вид связанного уведомления	УО	Заполняется в случае направления ранее в Банк России уведомления, связанного с текущим	[NTF_OWC] [NTF_ISI] [NTF_ORI] [NTF_CI] [NTF_CA] [NTF_VLN]	[NTF_OWC] – уведомление о выявленных случаях и (или) попытках осуществления переводов денежных средств без согласия клиента, а также о выявленных случаях и (или) попытках осуществления операций, направленных на совершение финансовых сделок с использованием финансовой платформы без волеизъявления участника финансовой платформы [NTF_ISI] – уведомление о выявлении инцидента защиты информации или результатах расследования инцидента защиты информации [NTF_ORI] – уведомление о выявлении инцидента операционной надежности или о результатах расследования инцидента операционной надежности [NTF_CI] – уведомление о компьютерных инцидентах [NTF_CA] – уведомления о компьютерных атаках [NTF_VLN] – уведомление о выявленных уязвимостях

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
33		Тип связи с другими уведомлениями			[Предшествующее событие] [Дочернее событие] [Связанное событие] [Уточнение сведений о событии]	-
34		Регистрационный номер уведомления			В соответствии с форматом АСОИ ФинЦЕРТ	Идентификатор уведомления или ответа на запрос, ранее направленного в ФинЦЕРТ участником информационного обмена
35	Ограничительный маркер TLP	Ограничительный маркер на распространение сведений из данного уведомления	Н	-	[TLP: WHITE] [TLP: GREEN] [TLP: AMBER] [TLP: RED]	В соответствии с обозначениями, принятыми в протоколе TLP. По умолчанию [TLP: GREEN], если не указано иное
36	Необходимость привлечения ФинЦЕРТ	Необходимость привлечения ФинЦЕРТ для устранения последствий компьютерного инцидента	УО	При необходимости	[Да]	-

Форма представления данных NTF_CI_SIM – Форма представления данных о компьютерном инциденте, связанном с изменением (подменой) идентификатора мобильного абонента (IMSI), идентификатора мобильного оборудования (IMEI) или сим-карты

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип уведомления	Тип уведомления	О	-	[NTF_CI_SIM]	Предзаполненное поле
2	Описание компьютерного инцидента	Описание компьютерного инцидента	Н	-	Текстовое поле	Текстовое описание компьютерного инцидента (в том числе дополнительные сведения о способе реализации КИ, способе выявления КИ и т. д.). В случае если компьютерный инцидент был выявлен с использованием сведений бюллетеня Банка России или НКЦКИ, необходимо указать номер данного бюллетеня
3	Классификация компьютерного инцидента	Вектор	О	-	[EXT]	Предзаполненное поле
4		Тип компьютерного инцидента	О	-	[SIM]	Предзаполненное поле
5	Дата и время обнаружения	Дата и время выявления компьютерного инцидента	О	-	В соответствии с RFC 3339	По московскому времени [UTC +03:00]
6	Сведения об объектах вредоносной активности, вызвавших компьютерный инцидент	Абонентский номер подвижной радиотелефонной связи	О	-	В соответствии с российской системой и планом нумерации	-
7		IMSI	О	-	Текстовое поле	-
8		Оператор связи	Н	-	Текстовое поле	-
9		Дата смены IMSI	Н	-	Текстовое поле	-
10	Оценка последствий компьютерного инцидента	Влияние на конфиденциальность	УО	При наличии указанных последствий	[Высокое] [Низкое]	-
11		Влияние на целостность			[Высокое] [Низкое]	-

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
12		Влияние на доступность			[Высокое] [Низкое]	-
13	Предпринятые меры по реагированию на компьютерный инцидент	Описание предпринятых действий в ходе реагирования на компьютерный инцидент	Н	-	Текстовое поле	-
14	Связь с другими уведомлениями	Вид связанного уведомления	УО	Заполняется в случае направления ранее в Банк России уведомления, связанного с текущим	[NTF_OWC] [NTF_ISI] [NTF_ORI] [NTF_CI] [NTF_CA] [NTF_VLN]	[NTF_OWC] – уведомление о выявленных случаях и (или) попытках осуществления переводов денежных средств без согласия клиента, а также о выявленных случаях и (или) попытках осуществления операций, направленных на совершение финансовых сделок с использованием финансовой платформы без волеизъявления участника финансовой платформы [NTF_ISI] – уведомление о выявлении инцидента защиты информации или результатах расследования инцидента защиты информации [NTF_ORI] – уведомление о выявлении инцидента операционной надежности или о результатах расследования инцидента операционной надежности [NTF_CI] – уведомление о компьютерных инцидентах [NTF_CA] – уведомления о компьютерных атаках [NTF_VLN] – уведомление о выявленных уязвимостях
15		Тип связи с другими уведомлениями			[Предшествующее событие] [Дочернее событие] [Связанное событие] [Уточнение сведений о событии]	-
16		Регистрационный номер уведомления			В соответствии с форматом АСОИ ФинЦЕРТ	Идентификатор уведомления или ответа на запрос, ранее направленного в ФинЦЕРТ участником информационного обмена
17	Ограничительный маркер TLP	Ограничительный маркер на распространение сведений из данного уведомления	Н	-	[TLP: WHITE] [TLP: GREEN] [TLP: AMBER] [TLP: RED]	В соответствии с обозначениями, принятыми в протоколе TLP. По умолчанию [TLP: GREEN], если не указано иное
18	Необходимость привлечения ФинЦЕРТ	Необходимость привлечения ФинЦЕРТ для устранения последствий компьютерного инцидента	УО	При необходимости	[Да]	-

Форма представления данных Attack_using_resource – Форма представления данных о компьютерном инциденте, связанном с использованием контролируемого ресурса для проведения атак

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип уведомления	Тип уведомления	О	-	[NTF_CI_Attack_using_resource]	Предзаполненное поле

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
2	Описание компьютерного инцидента	Описание компьютерного инцидента	Н	-	Текстовое поле	Текстовое описание компьютерного инцидента (в том числе дополнительные сведения о способе реализации КИ, способе выявления КИ и т. д.). В случае если компьютерный инцидент был выявлен с использованием сведений бюллетеня Банка России или НКЦКИ, необходимо указать номер данного бюллетеня
3	Классификация компьютерного инцидента	Вектор	О	-	[INT]	Предзаполненное поле
4		Тип компьютерного инцидента	О	-	[Attack using resource]	Предзаполненное поле
5	Дата и время обнаружения	Дата и время выявления компьютерного инцидента	О	-	В соответствии с RFC 3339	По московскому времени [UTC +03:00]
6	Сведения об объектах, на которые направлен компьютерный инцидент	Наименование контролируемого ресурса	О	-	Текстовое поле	-
7		Категория контролируемого ресурса	УО	Если является объектом КИИ	[Без категории значимости] [Третья категория значимости] [Вторая категория значимости] [Первая категория значимости]	-
8		Код уровня объекта/субъекта	О	-	Из классификатора «Типы объектов и субъектов», приведенного в приложении 28	-
9		Код типа объекта/субъекта	О	-	Перечень зависит от поля «Код уровня атакуемого объекта/субъекта». Из классификатора «Типы объектов и субъектов», приведенного в приложении 28	-
10		Наличие подключения к сети Интернет	О	-	[Да]	Предзаполненное поле
11		Страна/регион	О	-	В формате ISO-3166-2	-
12		IPv4-адрес контролируемого ресурса	УО	Обязательно заполнение одного из полей	Список IP-адресов	-
13		IPv6-адрес контролируемого ресурса				
14		Доменное имя контролируемого ресурса			Список доменных имен	
15		URI-адрес контролируемого ресурса			Список URI-адресов	
16		e-mail-адрес контролируемого объекта			Список e-mail-адресов	
17		Атакованная сетевая служба и порт/протокол	УО	При наличии соответствующей информации	Текстовое поле	-

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
18	Сведения об объектах вредоносной активности, вызвавших компьютерный инцидент	IPv4-адрес вредоносного объекта	УО	Выявлен IPv4-адрес вредоносного объекта	Список IP-адресов	-
19		IPv6-адрес вредоносного объекта		Выявлен IPv6-адрес вредоносного объекта		-
20		Доменное имя вредоносного объекта		Выявлено доменное имя вредоносного объекта	Список доменных имен	-
21		URI-адрес вредоносного объекта		Выявлен URI-адрес вредоносного объекта	Список URI-адресов	-
22		e-mail-адрес вредоносного объекта или субъекта		Выявлен e-mail-адрес вредоносного объекта или субъекта	Список e-mail-адресов	-
23		Уязвимость	УО	В случае если выявленная уязвимость описана в какой-либо системе описания уязвимостей	Перечень эксплуатируемых уязвимостей безопасности программного или аппаратного обеспечения, из соответствующего каталога (например, CVE, БДУ ФСТЭК и т. д.)	Обязательно заполняется один из блоков
24		Наименование системы описания уязвимостей			Текстовое поле	
25		Описание уязвимости	УО	В случае если выявленная уязвимость не описана ни в одной системе описания уязвимостей	Текстовое поле	
26		Описание объекта информатизации, в котором была проэксплуатирована уязвимость	О	-	В формате, соответствующем рекомендациям Банка России, опубликованным на официальном сайте	-
27		Файл ВПО	УО	Обязательно заполняется одно из полей	Файл	-
28		URL для скачивания			Текстовое поле	-
29		Хеш-сумма	О	-	Текстовое поле	-
30		Алгоритм хеширования		-	[SHA256] [SHA1] [MD5]	-
31	Оценка последствий компьютерного инцидента	Влияние на конфиденциальность	УО	При наличии указанных последствий	[Высокое] [Низкое]	-
32		Влияние на целостность			[Высокое] [Низкое]	-
33		Влияние на доступность			[Высокое] [Низкое]	-
34	Предпринятые меры по реагированию на компьютерный инцидент	Описание предпринятых действий в ходе реагирования на компьютерный инцидент	Н	-	Текстовое поле	-

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
35	Связь с другими уведомлениями	Вид связанного уведомления	УО	Заполняется в случае направления ранее в Банк России уведомления, связанного с текущим	[NTF_OWC] [NTF_ISI] [NTF_ORI] [NTF_CI] [NTF_CA] [NTF_VLN]	[NTF_OWC] – уведомление о выявленных случаях и (или) попытках осуществления переводов денежных средств без согласия клиента, а также о выявленных случаях и (или) попытках осуществления операций, направленных на совершение финансовых сделок с использованием финансовой платформы без волеизъявления участника финансовой платформы [NTF_ISI] – уведомление о выявлении инцидента защиты информации или результатах расследования инцидента защиты информации [NTF_ORI] – уведомление о выявлении инцидента операционной надежности или о результатах расследования инцидента операционной надежности [NTF_CI] – уведомление о компьютерных инцидентах [NTF_CA] – уведомления о компьютерных атаках [NTF_VLN] – уведомление о выявленных уязвимостях
36		Тип связи с другими уведомлениями			[Предшествующее событие] [Дочернее событие] [Связанное событие] [Уточнение сведений о событии]	-
37		Регистрационный номер уведомления			В соответствии с форматом АСОИ ФинЦЕРТ	Идентификатор уведомления или ответа на запрос, ранее направленного в ФинЦЕРТ участником информационного обмена
38	Ограничительный маркер TLP	Ограничительный маркер на распространение сведений из данного уведомления	Н	-	[TLP: WHITE] [TLP: GREEN] [TLP: AMBER] [TLP: RED]	В соответствии с обозначениями, принятыми в протоколе TLP. По умолчанию [TLP: GREEN], если не указано иное
39	Необходимость привлечения ФинЦЕРТ	Необходимость привлечения ФинЦЕРТ для устранения последствий компьютерного инцидента	УО	При необходимости	[Да]	-

Форма представления данных NTF_CI_Without_attack – Форма представления данных о компьютерном инциденте, не связанном с компьютерной атакой

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип уведомления	Тип уведомления	О	-	[NTF_CI_Without_attack]	Предзаполненное поле

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
2	Описание компьютерного инцидента	Описание компьютерного инцидента	Н	-	Текстовое поле	Текстовое описание компьютерного инцидента (в том числе дополнительные сведения о способе реализации КИ, способе выявления КИ и т. д.). В случае если компьютерный инцидент был выявлен с использованием сведений бюллетеня Банка России или НКЦКИ, необходимо указать номер данного бюллетеня
3	Классификация компьютерного инцидента	Вектор	О	-	[INT]	Предзаполненное поле
4		Тип компьютерного инцидента	О	-	[Without_attack]	Предзаполненное поле
5	Дата и время обнаружения	Дата и время выявления компьютерного инцидента	О	-	В соответствии с RFC 3339	По московскому времени [UTC +03:00]
6	Сведения об объектах, на которые направлен компьютерный инцидент	Наименование контролируемого ресурса	О	-	Текстовое поле	-
7		Категория контролируемого ресурса	УО	Если является объектом КИИ	[Без категории значимости] [Третья категория значимости] [Вторая категория значимости] [Первая категория значимости]	-
8		Код уровня объекта/субъекта	О	-	Из классификатора «Типы объектов и субъектов», приведенного в приложении 28	-
9		Код типа объекта/субъекта	О	-	Перечень зависит от поля «Код уровня атакуемого объекта/субъекта». Из классификатора «Типы объектов и субъектов», приведенного в приложении 28	-
10		Наличие подключения к сети Интернет	О	-	[Да]/[Нет]	-
11		Страна/регион	О	-	В формате ISO-3166-2	-
12		IPv4-адрес контролируемого ресурса	УО	Обязательно заполнение одного из полей	Список IP-адресов	-
13		IPv6-адрес контролируемого ресурса				
14		Доменное имя контролируемого ресурса			Список доменных имен	
15		URI-адрес контролируемого ресурса			Список URI-адресов	
16		e-mail-адрес контролируемого объекта			Список e-mail-адресов	
17	Оценка последствий компьютерного инцидента	Влияние на конфиденциальность	УО	При наличии указанных последствий	[Высокое] [Низкое]	-
18		Влияние на целостность			[Высокое] [Низкое]	-

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
19		Влияние на доступность			[Высокое] [Низкое]	-
20	Предпринятые меры по реагированию на компьютерный инцидент	Описание предпринятых действий в ходе реагирования на компьютерный инцидент	Н	-	Текстовое поле	-
21	Связь с другими уведомлениями	Вид связанного уведомления	УО	Заполняется в случае направления ранее в Банк России уведомления, связанного с текущим	[NTF_OWC] [NTF_ISI] [NTF_ORI] [NTF_CI] [NTF_CA] [NTF_VLN]	[NTF_OWC] – уведомление о выявленных случаях и (или) попытках осуществления переводов денежных средств без согласия клиента, а также о выявленных случаях и (или) попытках осуществления операций, направленных на совершение финансовых сделок с использованием финансовой платформы без волеизъявления участника финансовой платформы [NTF_ISI] – уведомление о выявлении инцидента защиты информации или результатах расследования инцидента защиты информации [NTF_ORI] – уведомление о выявлении инцидента операционной надежности или о результатах расследования инцидента операционной надежности [NTF_CI] – уведомление о компьютерных инцидентах [NTF_CA] – уведомления о компьютерных атаках [NTF_VLN] – уведомление о выявленных уязвимостях
22		Тип связи с другими уведомлениями			[Предшествующее событие] [Дочернее событие] [Связанное событие] [Уточнение сведений о событии]	-
23		Регистрационный номер уведомления			В соответствии с форматом АСОИ ФинЦЕРТ	Идентификатор уведомления или ответа на запрос, ранее направленного в ФинЦЕРТ участником информационного обмена
24	Ограничительный маркер TLP	Ограничительный маркер на распространение сведений из данного уведомления	Н	-	[TLP: WHITE] [TLP: GREEN] [TLP: AMBER] [TLP: RED]	В соответствии с обозначениями, принятыми в протоколе TLP. По умолчанию [TLP: GREEN], если не указано иное
25	Необходимость привлечения ФинЦЕРТ	Необходимость привлечения ФинЦЕРТ для устранения последствий компьютерного инцидента	УО	При необходимости	[Да]	-

ПРИЛОЖЕНИЕ 21. ФОРМА ПРЕДСТАВЛЕНИЯ ДАННЫХ NTF_CA – ФОРМА ПРЕДСТАВЛЕНИЯ УЧАСТНИКАМИ ИНФОРМАЦИОННОГО ОБМЕНА ДАННЫХ О КОМПЬЮТЕРНЫХ АТАКАХ

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип уведомления	Тип уведомления	О	-	[NTF_CA]	Предзаполненное поле
2	Описание компьютерной атаки	Описание компьютерной атаки	Н	-	Текстовое поле	Текстовое описание компьютерной атаки (в том числе дополнительные сведения о способе реализации КА, способе выявления КА и т. д.). В случае если компьютерная атака была выявлена с использованием сведений бюллетеня Банка России или НКЦКИ, необходимо указать номер данного бюллетеня
3	Классификация компьютерной атаки	Вектор компьютерной атаки	О	-	[EXT] [INT]	В соответствии с классификатором компьютерных атак, приведенном в приложении 18
4		Тип компьютерной атаки	О	-	[DoS] [Exploit attempt] [Infection attempt] [Login attempt] [Phishing] [Social engineering] [Scanning]	В соответствии с классификатором компьютерных атак, приведенном в приложении 18
5	Дата	Дата, за которую осуществляется свод данных по компьютерным атакам	О	-	В соответствии с RFC 3339	По московскому времени [UTC +03:00]
6	Сведения об объектах КИИ, на которые направлены компьютерные атаки	Наименование контролируемого информационного ресурса	УО	Заполняется в случае выявления атак на объект КИИ	Текстовое поле	-
7		Категория контролируемого ресурса			[Без категории значимости] [Третья категория значимости] [Вторая категория значимости] [Первая категория значимости]	-
8		Страна/регион			В формате ISO-3166-2	-
9		IPv4-адрес атакованного ресурса			Список IP-адресов или файл	Обязательно заполнение одного из полей
10		IPv6-адрес атакованного ресурса				
11		Доменное имя атакованного ресурса			Список доменных имен или файл	
12		URI-адрес атакованного ресурса			Список URI-адресов или файл	
13		e-mail-адрес атакованного объекта			Список e-mail-адресов или файл	
14		Атакованная сетевая служба и порт/протокол			Текстовое поле	Заполняется при наличии сведений

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
15	Сведения об объектах или субъектах вредоносной активности	Набор данных	УО	Состав данных зависит от поля «Тип компьютерной атаки» и приведен на вкладке «Сведения об объектах ВА»		
16	Ограничительный маркер TLP	Ограничительный маркер на распространение сведений из данного уведомления	Н	-	[TLP: WHITE] [TLP: GREEN] [TLP: AMBER] [TLP: RED]	В соответствии с обозначениями, принятыми в протоколе TLP. По умолчанию [TLP: GREEN], если не указано иное

Наименование компьютерной атаки	Сведения об объектах или субъектах вредоносной активности				
	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
Компьютерная атака типа «Отказ в обслуживании»	IPv4-адрес вредоносного объекта	УО	Выявлен IPv4-адрес вредоносного объекта	Список IP-адресов или файл	Заполняется как минимум одно из полей. Указываются все выявленные источники вредоносной активности за период свода
	IPv6-адрес вредоносного объекта		Выявлен IPv6-адрес вредоносного объекта		
	Доменное имя вредоносного объекта		Выявлено доменное имя вредоносного объекта	Список доменных имен или файл	
	Количество уникальных (по связке источник атаки + атакуемая система) атак «отказ в обслуживании» за период свода	О	-	Число	-
Попытки эксплуатации уязвимости	IPv4-адрес вредоносного объекта	УО	Выявлен IPv4-адрес вредоносного объекта	Список IP-адресов или файл	Заполняется как минимум одно из полей. Указываются все выявленные источники вредоносной активности за период свода
	IPv6-адрес вредоносного объекта		Выявлен IPv6-адрес вредоносного объекта		
	Доменное имя вредоносного объекта		Выявлено доменное имя вредоносного объекта	Список доменных имен или файл	
	URI-адрес вредоносного объекта		Выявлен URI-адрес вредоносного объекта	Список URI-адресов или файл	
	e-mail-адрес вредоносного объекта или субъекта		Выявлен e-mail-адрес вредоносного объекта или субъекта	Список e-mail-адресов или файл	
	Перечень уязвимостей, в отношении которых были попытки эксплуатации	УО	В случае если выявленная уязвимость описана в какой-либо системе описания уязвимостей	Перечень эксплуатируемых уязвимостей безопасности программного или аппаратного обеспечения, из соответствующего каталога (например, CVE, БДУ ФСТЭК и т. д.)	Обязательно заполняется один из блоков
	Наименование системы описания уязвимостей			Текстовое поле	

Наименование компьютерной атаки	Сведения об объектах или субъектах вредоносной активности				
	Описание АСОИ UI	**Обязательность полей**	**Условие обязательности**	**Правило заполнения**	**Примечание**
	Описание уязвимостей	УО	В случае если выявленная уязвимость не описана ни в одной системе описания уязвимостей	Текстовое поле	
	Количество уникальных (по связке источник атаки + атакуемая система) попыток эксплуатации за период свода	О	-	Число	-
Попытки внедрения модулей ВПО	IPv4-адрес вредоносного объекта	УО	Выявлен IPv4-адрес вредоносного объекта	Список IP-адресов или файл	Указываются все выявленные источники вредоносной активности за период свода
	IPv6-адрес вредоносного объекта		Выявлен IPv6-адрес вредоносного объекта		
	Доменное имя вредоносного объекта		Выявлено доменное имя вредоносного объекта	Список доменных имен или файл	
	URI-адрес вредоносного объекта		Выявлен URI-адрес вредоносного объекта	Список URI-адресов или файл	
	e-mail-адрес вредоносного объекта или субъекта		Выявлен e-mail-адрес вредоносного объекта или субъекта	Список e-mail-адресов или файл	
	Файл ВПО	УО	Обязательно заполняется одно из полей	Файл	Заполняется как минимум для одного образца ВПО. Блок заполняется отдельно для каждого образца ВПО
	URL для скачивания			Текстовое поле	
	Хеш-сумма	Н	-	Текстовое поле	
	Алгоритм хеширования		-	[SHA256] [SHA1] [MD5]	
	Количество выявленных попыток внедрения ВПО за период свода	О	-	Число	-
Неуспешные попытки авторизации	IPv4-адрес вредоносного объекта	УО	Выявлен IPv4-адрес вредоносного объекта	Список IP-адресов или файл	Заполняется как минимум одно из полей. Указываются все выявленные источники вредоносной активности за период свода
	IPv6-адрес вредоносного объекта		Выявлен IPv6-адрес вредоносного объекта		
	Доменное имя вредоносного объекта		Выявлено доменное имя вредоносного объекта	Список доменных имен или файл	
	URI-адрес вредоносного объекта		Выявлено доменное имя вредоносного объекта	Список доменных имен или файл	
	Количество уникальных (по связке источник вредоносной активности + учетная запись) неуспешных попыток авторизации за период свода	О	-	Число	-

Наименование компьютерной атаки	Сведения об объектах или субъектах вредоносной активности				
	Описание АСОИ UI	**Обязательность полей**	**Условие обязательности**	**Правило заполнения**	**Примечание**
Выявление фишинговой рассылки или ресурса	IPv4-адрес вредоносного объекта	УО	Выявлен IPv4-адрес вредоносного объекта	Список IP-адресов или файл	Заполняется как минимум одно из полей. Указываются все выявленные источники вредоносной активности за период свода
	IPv6-адрес вредоносного объекта		Выявлен IPv6-адрес вредоносного объекта		
	Доменное имя вредоносного объекта		Выявлено доменное имя вредоносного объекта	Список доменных имен или файл	
	URI-адрес вредоносного объекта		Выявлен URI-адрес вредоносного объекта	Список URI-адресов или файл	
	e-mail-адрес вредоносного объекта или субъекта		Выявлен e-mail-адрес вредоносного объекта или субъекта	Список e-mail-адресов или файл	
	Дополнительная информация о технике реализации атак	Н	-	Текстовое поле	-
Попытки социальной инженерии	IPv4-адрес вредоносного объекта	УО	Выявлен IPv4-адрес вредоносного объекта	Список IP-адресов или файл	Заполняется как минимум одно из полей. Указываются все выявленные источники вредоносной активности за период свода
	IPv6-адрес вредоносного объекта		Выявлен IPv6-адрес вредоносного объекта		
	Доменное имя вредоносного объекта		Выявлено доменное имя вредоносного объекта	Список доменных имен или файл	
	URI-адрес вредоносного объекта		Выявлен URI-адрес вредоносного объекта	Список URI-адресов или файл	
	e-mail-адрес вредоносного объекта или субъекта		Выявлен e-mail-адрес вредоносного объекта	Список e-mail-адресов или файл	
	Номер мобильного телефона вредоносного субъекта		Выявлен номер мобильного телефона вредоносного субъекта	Список номеров мобильных телефонов или файл	
	Дополнительная информация о технике реализации атак с использованием социальной инженерии	Н	-	Текстовое поле	-
Сетевое сканирование контролируемого ресурса	IPv4-адрес вредоносного объекта	УО	Выявлен IPv4-адрес вредоносного объекта	Список IP-адресов или файл	Заполняется как минимум одно из полей. Указываются все выявленные источники вредоносной активности за период свода
	IPv6-адрес вредоносного объекта		Выявлен IPv6-адрес вредоносного объекта		
	Доменное имя вредоносного объекта		Выявлено доменное имя вредоносного объекта	Список доменных имен или файл	
	URI-адрес вредоносного объекта		Выявлен URI-адрес вредоносного объекта	Список URI-адресов или файл	
	Количество уникальных (по связке источник сканирования + сканируемая система) событий сканирования за период свода	О	-	Число	-

ПРИЛОЖЕНИЕ 22. ФОРМЫ ПРЕДСТАВЛЕНИЯ ДАННЫХ NTF_CA, ПРЕДЗАПОЛНЕННЫЕ ДЛЯ КОМПЬЮТЕРНЫХ АТАК

Код компьютерной атаки	Наименование компьютерной атаки
[DoS]	**Компьютерная атака типа «Отказ в обслуживании»**
[Exploit attempt]	**Попытки эксплуатации уязвимости**
[Infection attempt]	**Попытки внедрения модулей ВПО**
[Login attempt]	**Неуспешные попытки авторизации**
[Phishing]	**Выявление фишинговой рассылки или ресурса**
[Social engineering]	**Попытки социальной инженерии**
[Scanning]	**Сетевое сканирование контролируемого ресурса**

Форма представления данных NTF_CA_DoS – Форма представления данных о компьютерных атаках, связанных с компьютерными атаками типа «Отказ в обслуживании»

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип уведомления	Тип уведомления	О	-	[NTF_CA_DoS]	Предзаполненное поле
2	Описание компьютерной атаки	Описание компьютерной атаки	Н	-	Текстовое поле	Текстовое описание компьютерной атаки (в том числе дополнительные сведения о способе реализации КА, способе выявления КА и т. д.). В случае если компьютерная атака была выявлена с использованием сведений бюллетеня Банка России или НКЦКИ, необходимо указать номер данного бюллетеня
3	Классификация компьютерной атаки	Вектор компьютерной атаки	О	-	[INT]	Предзаполненное поле
4		Тип компьютерной атаки	О	-	[DoS]	Предзаполненное поле
5	Дата	Дата, за которую осуществляется свод данных по компьютерным атакам	О	-	В соответствии с RFC 3339	По московскому времени [UTC +03:00]
6	Сведения об объектах КИИ, на которые направлены компьютерные атаки	Наименование контролируемого информационного ресурса	УО	Заполняется в случае выявления атак на объект КИИ	Текстовое поле	-
7		Категория контролируемого ресурса			[Без категории значимости] [Третья категория значимости] [Вторая категория значимости] [Первая категория значимости]	-
8		Страна/регион			В формате ISO-3166-2	-
9		IPv4-адрес атакованного ресурса			Список IP-адресов или файл	Обязательно заполнение одного из полей

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
10		IPv6-адрес атакованного ресурса				
11		Доменное имя атакованного ресурса			Список доменных имен или файл	
12		URI-адрес атакованного ресурса			Список URI-адресов или файл	
13		e-mail-адрес атакованного объекта			Список e-mail-адресов или файл	
14		Атакованная сетевая служба и порт/протокол			Текстовое поле	Заполняется при наличии сведений
15	Сведения об объектах или субъектах вредоносной активности	IPv4-адрес вредоносного объекта	УО	Выявлен IPv4-адрес вредоносного объекта	Список IP-адресов или файл	Заполняется как минимум одно из полей. Указываются все выявленные источники вредоносной активности за период свода
16		IPv6-адрес вредоносного объекта		Выявлен IPv6-адрес вредоносного объекта		
17		Доменное имя вредоносного объекта		Выявлено доменное имя вредоносного объекта	Список доменных имен или файл	
18		Количество уникальных (по связке источник атаки + атакуемая система) атак «Отказ в обслуживании» за период свода	О	-	Число	-
19	Ограничительный маркер TLP	Ограничительный маркер на распространение сведений из данного уведомления	Н	-	[TLP: WHITE] [TLP: GREEN] [TLP: AMBER] [TLP: RED]	В соответствии с обозначениями, принятыми в протоколе TLP. По умолчанию [TLP: GREEN], если не указано иное

Форма представления данных NTF_CA_Exploit attempt – Форма представления данных о компьютерных атаках, связанных с попытками эксплуатации уязвимости

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип уведомления	Тип уведомления	О	-	[NTF_CA_Exploit attempt]	Предзаполненное поле
2	Описание компьютерной атаки	Описание компьютерной атаки	Н	-	Текстовое поле	Текстовое описание компьютерной атаки (в том числе дополнительные сведения о способе реализации КА, способе выявления КА и т. д.). В случае если компьютерная атака была выявлена с использованием сведений бюллетеня Банка России или НКЦКИ, необходимо указать номер данного бюллетеня.
3	Классификация компьютерной атаки	Вектор компьютерной атаки	О	-	[INT]	Предзаполненное поле
4		Тип компьютерной атаки	О	-	[Exploit attempt]	Предзаполненное поле
5	Дата	Дата, за которую осуществляется свод данных по компьютерным атакам	О	-	В соответствии с RFC 3339	По московскому времени [UTC +03:00]

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
6	Сведения об объектах КИИ, на которые направлены компьютерные атаки	Наименование контролируемого информационного ресурса	УО	Заполняется в случае выявления атак на объект КИИ	Текстовое поле	-
7		Категория контролируемого ресурса			[Без категории значимости] [Третья категория значимости] [Вторая категория значимости] [Первая категория значимости]	-
8		Страна/регион			В формате ISO-3166-2	-
9		IPv4-адрес атакованного ресурса			Список IP-адресов или файл	Обязательно заполнение одного из полей
10		IPv6-адрес атакованного ресурса				
11		Доменное имя атакованного ресурса			Список доменных имен или файл	
12		URI-адрес атакованного ресурса			Список URI-адресов или файл	
13		e-mail-адрес атакованного объекта			Список e-mail-адресов или файл	
14		Атакованная сетевая служба и порт/протокол			Текстовое поле	Заполняется при наличии сведений
15	Сведения об объектах или субъектах вредоносной активности	IPv4-адрес вредоносного объекта	УО	Выявлен IPv4-адрес вредоносного объекта	Список IP-адресов или файл	Заполняется как минимум одно из полей. Указываются все выявленные источники вредоносной активности за период свода
16		IPv6-адрес вредоносного объекта		Выявлен IPv6-адрес вредоносного объекта		
17		Доменное имя вредоносного объекта		Выявлено доменное имя вредоносного объекта	Список доменных имен или файл	
18		URI-адрес вредоносного объекта		Выявлен URI-адрес вредоносного объекта	Список URI-адресов или файл	
19		e-mail-адрес вредоносного объекта или субъекта		Выявлен e-mail-адрес вредоносного объекта или субъекта	Список e-mail-адресов или файл	
20		Перечень уязвимостей, в отношении которых были попытки эксплуатации	УО	В случае если выявленная уязвимость описана в какой-либо системе описания уязвимостей	Перечень эксплуатируемых уязвимостей безопасности программного или аппаратного обеспечения, из соответствующего каталога (например, CVE, БДУ ФСТЭК и т. д.)	Обязательно заполняется один из блоков
21		Наименование системы описания уязвимостей			Текстовое поле	
22		Описание уязвимостей	УО	В случае если выявленная уязвимость не описана ни в одной системе описания уязвимостей	Текстовое поле	

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
23		Количество уникальных (по связке источник атаки + атакуемая система) попыток эксплуатации за период свода	О	-	Число	-
24	Ограничительный маркер TLP	Ограничительный маркер на распространение сведений из данного уведомления	Н	-	[TLP: WHITE] [TLP: GREEN] [TLP: AMBER] [TLP: RED]	В соответствии с обозначениями, принятыми в протоколе TLP. По умолчанию [TLP: GREEN], если не указано иное

Форма представления данных NTF_CA_Infection attempt – Форма представления данных о компьютерных атаках, связанных с попытками внедрения модулей ВПО

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип уведомления	Тип уведомления	О	-	[NTF_CA_Infection attempt]	Предзаполненное поле
2	Описание компьютерной атаки	Описание компьютерной атаки	Н	-	Текстовое поле	Текстовое описание компьютерной атаки (в том числе дополнительные сведения о способе реализации КА, способе выявления КА и т. д.). В случае если компьютерная атака была выявлена с использованием сведений бюллетеня Банка России или НКЦКИ, необходимо указать номер данного бюллетеня
3	Классификация компьютерной атаки	Вектор компьютерной атаки	О	-	[EXT] [INT]	[EXT] – направлено на клиента или контрагента финансовой организации или иных взаимодействующих с финансовой организации лиц [INT] – направлено на объекты информатизации финансовой организации
4		Тип компьютерной атаки	О	-	[Infection attempt]	Предзаполненное поле
5	Дата	Дата, за которую осуществляется свод данных по компьютерным атакам	О	-	В соответствии с RFC 3339	По московскому времени [UTC +03:00]
6	Сведения об объектах КИИ, на которые направлены компьютерные атаки	Наименование контролируемого информационного ресурса	УО	Заполняется в случае выявления атак на объект КИИ	Текстовое поле	-
7		Категория контролируемого ресурса			[Без категории значимости] [Третья категория значимости] [Вторая категория значимости] [Первая категория значимости]	-
8		Страна/регион			В формате ISO-3166-2	-
9		IPv4-адрес атакованного ресурса			Список IP-адресов или файл	Обязательно заполнение одного из полей
10		IPv6-адрес атакованного ресурса				
11		Доменное имя атакованного ресурса			Список доменных имен или файл	

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
12		URI-адрес атакованного ресурса			Список URI-адресов или файл	
13		e-mail-адрес атакованного объекта			Список e-mail-адресов или файл	
14		Атакованная сетевая служба и порт/протокол			Текстовое поле	Заполняется при наличии сведений
15	Сведения об объектах или субъектах вредоносной активности	IPv4-адрес вредоносного объекта	УО	Выявлен IPv4-адрес вредоносного объекта	Список IP-адресов или файл	Указываются все выявленные источники вредоносной активности за период свода
16		IPv6-адрес вредоносного объекта		Выявлен IPv6-адрес вредоносного объекта		
17		Доменное имя вредоносного объекта		Выявлено доменное имя вредоносного объекта	Список доменных имен или файл	
18		URI-адрес вредоносного объекта		Выявлен URI-адрес вредоносного объекта	Список URI-адресов или файл	
19		e-mail-адрес вредоносного объекта или субъекта		Выявлен e-mail-адрес вредоносного объекта или субъекта	Список e-mail-адресов или файл	
20		Файл ВПО	УО	Обязательно заполняется одно из полей	Файл	Заполняется как минимум для одного образца ВПО. Блок заполняется отдельно для каждого образца ВПО
21		URL для скачивания			Текстовое поле	
22		Хеш-сумма	Н	-	Текстовое поле	
23		Алгоритм хеширования		-	[SHA256] [SHA1] [MD5]	
24		Количество выявленных попыток внедрения ВПО за период свода	О	-	Число	-
25	Ограничительный маркер TLP	Ограничительный маркер на распространение сведений из данного уведомления	Н	-	[TLP: WHITE] [TLP: GREEN] [TLP: AMBER] [TLP: RED]	В соответствии с обозначениями, принятыми в протоколе TLP. По умолчанию [TLP: GREEN], если не указано иное

Форма представления данных NTF_CA_Login attempt – Форма представления данных о компьютерных атаках, связанных с неуспешными попытками авторизации

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип уведомления	Тип уведомления	О	-	[NTF_CA_Login attempt]	Предзаполненное поле
2	Описание компьютерной атаки	Описание компьютерной атаки	Н	-	Текстовое поле	Текстовое описание компьютерной атаки (в том числе дополнительные сведения о способе реализации КА, способе выявления КА и т. д.). В случае если компьютерная атака была выявлена с использованием сведений бюллетеня Банка России или НКЦКИ, необходимо указать номер данного бюллетеня

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
3	Классификация компьютерной атаки	Вектор компьютерной атаки	О	-	[EXT] [INT]	[EXT] – направлено на клиента или контрагента финансовой организации или иных взаимодействующих с финансовой организации лиц [INT] – направлено на объекты информатизации финансовой организации
4		Тип компьютерной атаки	О	-	[Login attempt]	Предзаполненное поле
5	Дата	Дата, за которую осуществляется свод данных по компьютерным атакам	О	-	В соответствии с RFC 3339	По московскому времени [UTC +03:00]
6	Сведения об объектах КИИ, на которые направлены компьютерные атаки	Наименование контролируемого информационного ресурса	УО	Заполняется в случае выявления атак на объект КИИ	Текстовое поле	-
7		Категория контролируемого ресурса			[Без категории значимости] [Третья категория значимости] [Вторая категория значимости] [Первая категория значимости]	-
8		Страна/регион			В формате ISO-3166-2	-
9		IPv4-адрес атакованного ресурса			Список IP-адресов или файл	Обязательно заполнение одного из полей
10		IPv6-адрес атакованного ресурса				
11		Доменное имя атакованного ресурса			Список доменных имен или файл	
12		URI-адрес атакованного ресурса			Список URI-адресов или файл	
13		e-mail-адрес атакованного объекта			Список e-mail-адресов или файл	
14		Атакованная сетевая служба и порт/протокол			Текстовое поле	Заполняется при наличии сведений
15	Сведения об объектах или субъектах вредоносной активности	IPv4-адрес вредоносного объекта	УО	Выявлен IPv4-адрес вредоносного объекта	Список IP-адресов или файл	Заполняется как минимум одно из полей. Указываются все выявленные источники вредоносной активности за период свода
16		IPv6-адрес вредоносного объекта		Выявлен IPv6-адрес вредоносного объекта		
17		Доменное имя вредоносного объекта		Выявлено доменное имя вредоносного объекта	Список доменных имен или файл	
18		URI-адрес вредоносного объекта		Выявлено доменное имя вредоносного объекта	Список доменных имен или файл	
19		Количество уникальных (по связке источник вредоносной активности + учетная запись) неуспешных попыток авторизации за период свода	О	-	Число	-

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
20	Ограничительный маркер TLP	Ограничительный маркер на распространение сведений из данного уведомления	Н	-	[TLP: WHITE] [TLP: GREEN] [TLP: AMBER] [TLP: RED]	В соответствии с обозначениями, принятыми в протоколе TLP. По умолчанию [TLP: GREEN], если не указано иное

Форма представления данных NTF_CA_Phishing – Форма представления данных о компьютерных атаках, связанных с выявлением фишинговой рассылки или ресурса

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип уведомления	Тип уведомления	О	-	[NTF_CA_Phishing]	Предзаполненное поле
2	Описание компьютерной атаки	Описание компьютерной атаки	Н	-	Текстовое поле	Текстовое описание компьютерной атаки (в том числе дополнительные сведения о способе реализации КА, способе выявления КА и т. д.). В случае если компьютерная атака была выявлена с использованием сведений бюллетеня Банка России или НКЦКИ, необходимо указать номер данного бюллетеня
3	Классификация компьютерной атаки	Вектор компьютерной атаки	О	-	[EXT] [INT]	[EXT] – направлено на клиента или контрагента финансовой организации или иных взаимодействующих с финансовой организации лиц [INT] – направлено на объекты информатизации финансовой организации
4		Тип компьютерной атаки	О	-	[Phishing]	Предзаполненное поле
5	Дата	Дата, за которую осуществляется свод данных по компьютерным атакам	О	-	В соответствии с RFC 3339	По московскому времени [UTC +03:00]
6	Сведения об объектах КИИ, на которые направлены компьютерные атаки	Наименование контролируемого информационного ресурса	УО	Заполняется в случае выявления атак на объект КИИ	Текстовое поле	-
7		Категория контролируемого ресурса			[Без категории значимости] [Третья категория значимости] [Вторая категория значимости] [Первая категория значимости]	-
8		Страна/регион			В формате ISO-3166-2	-
9		IPv4-адрес атакованного ресурса			Список IP-адресов или файл	Обязательно заполнение одного из полей
10		IPv6-адрес атакованного ресурса				
11		Доменное имя атакованного ресурса			Список доменных имен или файл	
12		URI-адрес атакованного ресурса			Список URI-адресов или файл	
13		e-mail-адрес атакованного объекта			Список e-mail-адресов или файл	
14		Атакованная сетевая служба и порт/протокол			Текстовое поле	Заполняется при наличии сведений

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
15	Сведения об объектах или субъектах вредоносной активности	IPv4-адрес вредоносного объекта	УО	Выявлен IPv4-адрес вредоносного объекта	Список IP-адресов или файл	Заполняется как минимум одно из полей. Указываются все выявленные источники вредоносной активности за период свода
16		IPv6-адрес вредоносного объекта		Выявлен IPv6-адрес вредоносного объекта		
17		Доменное имя вредоносного объекта		Выявлено доменное имя вредоносного объекта	Список доменных имен или файл	
18		URI-адрес вредоносного объекта		Выявлен URI-адрес вредоносного объекта	Список URI-адресов или файл	
19		e-mail-адрес вредоносного объекта или субъекта		Выявлен e-mail-адрес вредоносного объекта или субъекта	Список e-mail-адресов или файл	
20		Дополнительная информация о технике реализации атак	Н	-	Текстовое поле	-
21	Ограничительный маркер TLP	Ограничительный маркер на распространение сведений из данного уведомления	Н	-	"[TLP: WHITE] [TLP: GREEN] [TLP: AMBER] [TLP: RED] "	В соответствии с обозначениями, принятыми в протоколе TLP. По умолчанию [TLP: GREEN], если не указано иное

Форма представления данных NTF_CA_Social engineering – Форма представления данных о компьютерных атаках, связанных с попытками социальной инженерии

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип уведомления	Тип уведомления	О	-	[NTF_CA_Social engineering]	Предзаполненное поле
2	Описание компьютерной атаки	Описание компьютерной атаки	Н	-	Текстовое поле	Текстовое описание компьютерной атаки (в том числе дополнительные сведения о способе реализации КА, способе выявления КА и т. д.). В случае если компьютерная атака была выявлена с использованием сведений бюллетеня Банка России или НКЦКИ, необходимо указать номер данного бюллетеня
3	Классификация компьютерной атаки	Вектор компьютерной атаки	О	-	[EXT] [INT]	[EXT] – направлено на клиента или контрагента финансовой организации или иных взаимодействующих с финансовой организации лиц [INT] – направлено на объекты информатизации финансовой организации
4		Тип компьютерной атаки	О	-	[Social engineering]	Предзаполненное поле

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
5	Дата	Дата, за которую осуществляется свод данных по компьютерным атакам	О	-	В соответствии с RFC 3339	По московскому времени [UTC +03:00]
6	Сведения об объектах КИИ, на которые направлены компьютерные атаки	Наименование контролируемого информационного ресурса	УО	Заполняется в случае выявления атак на объект КИИ	Текстовое поле	-
7		Категория контролируемого ресурса			[Без категории значимости] [Третья категория значимости] [Вторая категория значимости] [Первая категория значимости]	-
8		Страна/регион			В формате ISO-3166-2	-
9		IPv4-адрес атакованного ресурса			Список IP-адресов или файл	Обязательно заполнение одного из полей
10		IPv6-адрес атакованного ресурса				
11		Доменное имя атакованного ресурса			Список доменных имен или файл	
12		URI-адрес атакованного ресурса			Список URI-адресов или файл	
13		e-mail-адрес атакованного объекта			Список e-mail-адресов или файл	
14		Атакованная сетевая служба и порт/протокол			Текстовое поле	Заполняется при наличии сведений
15	Сведения об объектах или субъектах вредоносной активности	IPv4-адрес вредоносного объекта	УО	Выявлен IPv4-адрес вредоносного объекта	Список IP-адресов или файл	Заполняется как минимум одно из полей. Указываются все выявленные источники вредоносной активности за период свода
16		IPv6-адрес вредоносного объекта		Выявлен IPv6-адрес вредоносного объекта		
17		Доменное имя вредоносного объекта		Выявлено доменное имя вредоносного объекта	Список доменных имен или файл	
18		URI-адрес вредоносного объекта		Выявлен URI-адрес вредоносного объекта	Список URI-адресов или файл	
19		e-mail-адрес вредоносного объекта или субъекта		Выявлен e-mail-адрес вредоносного объекта	Список e-mail-адресов или файл	
20		Номер мобильного телефона вредоносного субъекта		Выявлен номер мобильного телефона вредоносного субъекта	Список номеров мобильных телефонов или файл	
21		Дополнительная информация о технике реализации атак с использованием социальной инженерии	Н	-	Текстовое поле	-

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
22	Ограничительный маркер TLP	Ограничительный маркер на распространение сведений из данного уведомления	Н	-	[TLP: WHITE] [TLP: GREEN] [TLP: AMBER] [TLP: RED]	В соответствии с обозначениями, принятыми в протоколе TLP. По умолчанию [TLP: GREEN], если не указано иное

Форма представления данных NTF_CA_Scanning – Форма представления данных о компьютерных атаках, связанных с сетевым сканированием контролируемого ресурса

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип уведомления	Тип уведомления	О	-	[NTF_CA_Scanning]	Предзаполненное поле
2	Описание компьютерной атаки	Описание компьютерной атаки	Н	-	Текстовое поле	Текстовое описание компьютерной атаки (в том числе дополнительные сведения о способе реализации КА, способе выявления КА и т. д.). В случае если компьютерная атака была выявлена с использованием сведений бюллетеня Банка России или НКЦКИ, необходимо указать номер данного бюллетеня
3	Классификация компьютерной атаки	Вектор компьютерной атаки	О	-	[INT]	Предзаполненное поле
4		Тип компьютерной атаки	О	-	[Scanning]	Предзаполненное поле
5	Дата	Дата, за которую осуществляется свод данных по компьютерным атакам	О	-	В соответствии с RFC 3339	По московскому времени [UTC +03:00]
6	Сведения об объектах КИИ, на которые направлены компьютерные атаки	Наименование контролируемого информационного ресурса	УО	Заполняется в случае выявления атак на объект КИИ	Текстовое поле	-
7		Категория контролируемого ресурса			[Без категории значимости] [Третья категория значимости] [Вторая категория значимости] [Первая категория значимости]	-
8		Страна/регион			В формате ISO-3166-2	-
9		IPv4-адрес атакованного ресурса			Список IP-адресов или файл	Обязательно заполнение одного из полей
10		IPv6-адрес атакованного ресурса				
11		Доменное имя атакованного ресурса			Список доменных имен или файл	
12		URI-адрес атакованного ресурса			Список URI-адресов или файл	
13		e-mail-адрес атакованного объекта			Список e-mail-адресов или файл	
14		Атакованная сетевая служба и порт/протокол			Текстовое поле	Заполняется при наличии сведений

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
15	Сведения об объектах или субъектах вредоносной активности	IPv4-адрес вредоносного объекта	УО	Выявлен IPv4-адрес вредоносного объекта	Список IP-адресов или файл	Заполняется как минимум одно из полей. Указываются все выявленные источники вредоносной активности за период свода
16		IPv6-адрес вредоносного объекта		Выявлен IPv6-адрес вредоносного объекта		
17		Доменное имя вредоносного объекта		Выявлено доменное имя вредоносного объекта	Список доменных имен или файл	
18		URI-адрес вредоносного объекта		Выявлен URI-адрес вредоносного объекта	Список URI-адресов или файл	
19		Количество уникальных (по связке источник сканирования + сканируемая система) событий сканирования за период свода	О	-	Число	-
20	Ограничительный маркер TLP	Ограничительный маркер на распространение сведений из данного уведомления	Н	-	[TLP: WHITE] [TLP: GREEN] [TLP: AMBER] [TLP: RED]	В соответствии с обозначениями, принятыми в протоколе TLP. По умолчанию [TLP: GREEN], если не указано иное

ПРИЛОЖЕНИЕ 23. ФОРМА ПРЕДСТАВЛЕНИЯ ДАННЫХ NTF_VULNERABILITIES – ФОРМА ПРЕДСТАВЛЕНИЯ УЧАСТНИКАМИ ИНФОРМАЦИОННОГО ОБМЕНА ДАННЫХ О ВЫЯВЛЕННЫХ УЯЗВИМОСТЯХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Порядковый номер	Категория элемента данных		Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип уведомления		Тип уведомления	О	-	[NTF_Vulnerabilities]	Предзаполненное поле
2	Общая информация о проведенном анализе уязвимостей		Дата проведения анализа уязвимостей	О	-	В соответствии с RFC 3339	По московскому времени [UTC +03:00]
3			Организация, проводившая анализ уязвимостей	О	-	Наименование организации, проводившей анализ уязвимостей, или [Самостоятельно]	-
4	Результаты проведенного анализа уязвимостей (заполняется отдельно для каждого объекта информатизации, в котором была выявлена уязвимость)	Описание объекта информатизации, в котором выявлена уязвимость	Уровень объекта информатизации, в котором выявлена уязвимость	О	-	Из классификатора «Типы объектов и субъектов», приведенного в приложении 28	-
5			Тип объекта информатизации, в котором выявлена уязвимость	О	-	Из классификатора «Типы объектов и субъектов», приведенного в приложении 28	Перечень зависит от поля «Уровень объекта информатизации, в котором выявлена уязвимость»
6			Объект информатизации, в котором выявлена уязвимость в формате CPE	О	-	В формате, соответствующем рекомендациям Банка России, опубликованном на официальном сайте	-
7			Категория контролируемого ресурса	УО	Если является объектом КИИ	[Без категории значимости] [Третья категория значимости] [Вторая категория значимости] [Первая категория значимости]	-
8			Наличие подключения к сети Интернет	О	-	[Да]/[Нет]	-
9		Технические сведения объекта информатизации, в котором выявлена уязвимость	IPv4-адрес (маршрутизируемый) объекта информатизации	УО	Заполняются поля, идентифицирующие конкретный объект информатизации	Текстовое поле	Обязательно заполняется хотя бы один из элементов
10			IPv6-адрес (маршрутизируемый) объекта информатизации			Текстовое поле	
11			Доменное имя, ассоциированное с объектом информатизации			Текстовое поле	
12			URI-адрес объекта информатизации			Текстовое поле	
13			Номер атакованной автономной системы (ASN)			Текстовое поле	

Порядковый номер	Категория элемента данных		Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
14		Описание выявленных уязвимостей (заполняется отдельно для каждой уязвимости, выявленной в объекте информатизации)	Уязвимость объекта информатизации	УО	В случае если выявленная уязвимость описана в системе описания уязвимостей	Текстовое поле При использовании нескольких уязвимостей безопасности перечисляются через «+»	Обязательно заполняется один из блоков
15			Наименование системы описания уязвимостей			[CVE] [БДУ ФСТЭК]	
16			Описание уязвимости	УО	В случае если выявленная уязвимость не описана ни в одной системе описания уязвимостей	Текстовое поле	
17		Предпринятые меры по устранению выявленных уязвимостей	Статус устранения выявленных слабостей и уязвимостей объекта информатизации	О	-	[Fixed] [inProcess]	[Fixed] – меры приняты, уязвимость устранена [inProcess] – проводятся мероприятия по устранению уязвимости
18			Предпринятые меры по устранению уязвимости	УО	«Статус устранения выявленных слабостей и уязвимостей объекта информатизации» = [Fixed]	Текстовое поле	Подробное описание принятых мер для устранения уязвимости

ПРИЛОЖЕНИЕ 24. ФОРМА ПРЕДСТАВЛЕНИЯ ДАННЫХ REQ_IEP_DETECT – ФОРМА ЗАПРОСА БАНКА РОССИИ В ЦЕЛЯХ ПОЛУЧЕНИЯ СВЕДЕНИЙ О ВЫЯВЛЕННОЙ КОМПЬЮТЕРНОЙ АТАКЕ ИЛИ УЯЗВИМОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип запроса/ответа	Тип запроса/ответа	О	-	[REQ_IEP_Detect]	Предзаполненное поле
2	Тип события	Тип выявленного события	О	-	[Зараженный ресурс] [Источник e-mail-рассылки модулей ВПО] [Источник распространения модулей ВПО] [Центр управления ВПО] [Элемент инфраструктуры ВПО] [Замедление работы ресурса] [Источник эксплуатации уязвимости] [Источник компрометации учетной записи] [Участник захвата сетевого трафика] [Источник несанкционированного доступа] [Источник несанкционированного изменения информации] [Источник рассылки спам-сообщений] [Публикация запрещенной законодательством РФ информации] [Размещение фишингового ресурса] [Наличие несанкционированного контента] [Участник DDoS-атаки] [Скомпрометированная учетная запись] [Источник сетевого сканирования] [Участник мошеннической деятельности] [Источник угрозы социальной инженерии] [Уязвимый ресурс] [Подозрение на фишинговый ресурс] [Угроза компрометации ПДн] [Угроза компьютерной атаки]	-
3	Описание события информационной безопасности	Описание выявленного события информационной безопасности	Н	-	Текстовое поле	Текстовое описание выявленного события информационной безопасности
4	Дата и время события информационной безопасности	Дата и время выявления события информационной безопасности	О	-	В соответствии с RFC 3339	По московскому времени [UTC +03:00]
5		Дата и время завершения события информационной безопасности	УО	При наличии	В соответствии с RFC 3339	По московскому времени [UTC +03:00]

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
6	Владелец информационного ресурса	Владелец информационного ресурса	О	-	Текстовое поле	-
7	Сведения об объектах, на которые направлено событие информационной безопасности	IPv4-адрес атакованного ресурса	УО	При наличии соответствующей информации	Список IP-адресов	-
8		IPv6-адрес атакованного ресурса				
9		Доменное имя атакованного ресурса			Список доменных имен	
		Наименование регистратора домена			Список наименований регистраторов домена	
10		URI-адрес атакованного ресурса			Список URI-адресов	
11		e-mail-адрес атакованного объекта			Список e-mail-адресов	
12		Атакованная сетевая служба и порт/протокол			Текстовое поле	-
13		AS-Path до атакованной Автономной системы (ASN)			Текстовое поле	
14	Сведения об объектах вредоносной активности, вызвавших событие информационной безопасности	IPv4-адрес вредоносного объекта	УО	Выявлен IPv4-адрес вредоносного объекта	Список IP-адресов	-
15		IPv6-адрес вредоносного объекта		Выявлен IPv6-адрес вредоносного объекта		-
16		Доменное имя вредоносного объекта		Выявлено доменное имя вредоносного объекта	Список доменных имен	-
		Наименование регистратора домена			Список наименований регистраторов домена	
17		URI-адрес вредоносного объекта		Выявлен URI-адрес вредоносного объекта	Список URI-адресов	-
18		e-mail-адрес вредоносного объекта или субъекта		Выявлен e-mail-адрес вредоносного объекта или субъекта	Список e-mail-адресов	-
19		Файл ВПО	УО	Обязательно заполняется одно из полей	Файл	-
20		URL для скачивания			Текстовое поле	-
21		Хеш-сумма	О	-	Текстовое поле	-
22		Алгоритм хеширования		-	[SHA256] [SHA1] [MD5]	-
23		Уязвимость	УО	В случае если выявлен факт эксплуатации уязвимостей ВПО	Перечень эксплуатируемых уязвимостей безопасности программного или аппаратного обеспечения из соответствующего каталога (например, CVE, БДУ ФСТЭК и т. д.)	-

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
24		Наименование системы описания уязвимостей			Текстовое поле	-
25		Описание уязвимости, не описанной ни в одной системе описания уязвимостей			Текстовое поле	-
26		Номер подставной Автономной системы (ASN)	O	-	Текстовое поле	-
27		Наименование AS	O	-	Текстовое поле	-
28		Наименование LIR	O	-	Текстовое поле	-
29	Ограничительный маркер TLP	Ограничительный маркер на распространение сведений из данного уведомления	H	-	[TLP: WHITE] [TLP: GREEN] [TLP: AMBER] [TLP: RED]	В соответствии с обозначениями, принятыми в протоколе TLP. По умолчанию [TLP: GREEN], если не указано иное

Форма представления данных RESP_IEP_Detect – Форма представления ответа на запрос Банка России в целях получения сведений о выявленной компьютерной атаке или уязвимости информационной безопасности

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип запроса/ответа	Тип запроса/ответа	O	-	[RESP_IEP_Detect]	Предзаполненное поле
2	Результат принятого решения	Результат принятого решения	O	-	[Меры приняты] [Информация учтена] [Сведения не подтверждены]	-

ПРИЛОЖЕНИЕ 25. ФОРМА ПРЕДСТАВЛЕНИЯ ДАННЫХ REQ_IEP_ISWEBSITE – ФОРМА ЗАПРОСА БАНКА РОССИИ В ЦЕЛЯХ ПОЛУЧЕНИЯ СВЕДЕНИЙ О ПРИНАДЛЕЖНОСТИ УЧАСТНИКУ ИНФОРМАЦИОННОГО ОБМЕНА РЕСУРСА В СЕТИ ИНТЕРНЕТ

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип запроса/ответа	Тип запроса/ответа	О	-	[INQ_WEB_REQ]	Предзаполненное поле
2	Общие данные запроса	Описание	О	-	Текстовое поле	-
3		Правовое обоснование	О	-	Текстовое поле	-
4		URL-адрес ресурса	УО	Заполняется по крайней мере одно поле	Текстовое поле	-
5		IP-адрес ресурса	УО		Текстовое поле	-
6		Доменное имя атакованного ресурса	УО		Текстовое поле	-
7		Осуществляется распространение ВПО, фишинговой информации или запрещенной законодательством РФ информации	УО	Если осуществляется распространение ВПО, фишинговой информации или запрещенной законодательством РФ информации	[Да]	-

Форма представления данных RESP_IEP_IsWebSite – Форма представления ответа на запрос Банка России в целях получения сведений о принадлежности участнику информационного обмена ресурса в сети Интернет

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип запроса/ответа	Тип запроса/ответа	О	-	[INQ_WEB_RESP]	Предзаполненное поле
2	Общие данные ответа на запрос	Принадлежность к организации	О	-	[Да] [Нет]	-
3		URL-адрес ресурса	УО	«Принадлежность к организации» = [Да]	Текстовое поле	Заполняются поля, которые не были заполнены во входящем запросе
4		IP-адрес ресурса	УО		Текстовое поле	
5		Доменное имя атакованного ресурса	УО		Текстовое поле	
6		Описание мер по устранению распространения ВПО	УО	«Принадлежность к организации» = [Да]	Текстовое поле	-
7		Является ли, по мнению организации, указанный ресурс распространяющим ВПО, фишинговую информацию или запрещенную законодательством РФ информацию	УО	«Принадлежность к организации» = [Нет]	[Да] [Нет]	-
8		Согласие на принятие Банком России мер по блокировке в отношении данного ресурса	УО	«Принадлежность к организации» = [Нет]	[Да] [Нет]	-

ПРИЛОЖЕНИЕ 26. ФОРМА ПРЕДСТАВЛЕНИЯ ДАННЫХ REQ_IEP_CORRACCLOCK – ФОРМА ПРЕДСТАВЛЕНИЯ ДАННЫХ, ИСПОЛЬЗУЕМАЯ ДЛЯ ЗАПРОСА В БАНК РОССИИ УЧАСТНИКАМИ ИНФОРМАЦИОННОГО ОБМЕНА, ИСПОЛЬЗУЮЩИХ СЕРВИС СРОЧНОГО ПЕРЕВОДА И СЕРВИС НЕСРОЧНОГО ПЕРЕВОДА ДЛЯ ОСУЩЕСТВЛЕНИЯ ПЕРЕВОДА ДЕНЕЖНЫХ СРЕДСТВ, НЕ ЯВЛЯЮЩИХСЯ ПОДРАЗДЕЛЕНИЯМИ БАНКА РОССИИ, ОБ УСТАНОВЛЕНИИ (ИЛИ СНЯТИИ) НА ИХ БАНКОВСКИЕ (КОРРЕСПОНДЕНТСКИЕ) СЧЕТА (СУБСЧЕТА) ОГРАНИЧЕНИЯ В ВИДЕ ЗАПРЕТА НА СПИСАНИЕ ДЕНЕЖНЫХ СРЕДСТВ ПРИ ВЫЯВЛЕНИИ ИНЦИДЕНТОВ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ОСУЩЕСТВЛЕНИИ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ, НА ОБЪЕКТАХ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ УЧАСТНИКОВ ИНФОРМАЦИОННОГО ОБМЕНА

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип запроса/ответа	Тип запроса/ответа	O	-	[REQ_IEP_CorrAccLock]	Предзаполненное поле
2	Используемая система	Тип системы	O	-	Выбор одного из значений: [PSBR] [SPFS]	[PSBR] – платежная система Банка России [SPFS] – система передачи финансовых сообщений Банка России
3	Тип участника	Тип участника	O	«Тип системы» = [SPFS]	Выбор одного из значений: [AGT] [STDALN_MEMBER] [SERV_BR] [CSTSERV_BR]	[AGT] – агент. Юридическое лицо – пользователь СПФС, заключившее с Банком России договор, содержащий условия о предоставлении Банком России услуг по передаче финансовых сообщений и условия передачи финансовой информации третьих лиц через СПФС (обособленных пользователей (клиентов сервис-бюро) [STDALN_MEMBER]/[SERV_BR] – обособленный пользователь СПФС/Сервис-бюро. Пользователь СПФС, который состоит в договорных отношениях с пользователем СПФС, имеющим право на передачу финансовой информации третьих лиц (агент). [CSTSERV_BR] – клиент сервис-бюро – юридическое лицо, заключившее с сервис-бюро договор передачи финансовых сообщений через СПФС
4	Общие сведения	УИС	O	-	Текстовое поле	-
5		Регистрационный номер	O	«Тип системы» = [PSBR]	Текстовое поле	-
6		БИК участника	O	«Тип системы» = [PSBR]	Текстовое поле	-

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
7		Операция	O	-	Выбор одного из значений: [ON] [OFF]	[ON] – в случае установления на банковские (корреспондентские) счета (субсчета) ограничения в виде запрета на списание денежных средств или приостановление обмена электронными финансовыми сообщениями через СПФС [OFF] – в случае снятия установления на банковские (корреспондентские) счета (субсчета) ограничения в виде запрета на списание денежных средств или снятие ограничений на обмен электронными финансовыми сообщениями в СПФС
8		Дата исполнения операции	O	-	Дата и время в формате: dd.mm.yyyy hh: mm	[UTC +03:00]
9		Описание	H	-	Текстовое поле	-
10		Вложение	O	-	Файл	-
11	Контактное лицо	Фамилия	O	-	Текстовое поле	-
12		Имя	O	-	Текстовое поле	-
13		Отчество	O	-	Текстовое поле	-
14		Должность	O	-	Текстовое поле	-
15		e-mail-адрес	O	-	Текстовое поле	-
16		Городской телефон	O	-	Текстовое поле	-
17		Мобильный телефон	O	-	Текстовое поле	-

Форма представления данных RESP_IEP_CorrAccLock – Форма представления данных, используемая Банком России для информационного сообщения об установлении (или снятии) на банковские (корреспондентские) счета (субсчета) участников информационного обмена ограничения в виде запрета на списание денежных средств

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип запроса/ответа	Тип запроса/ответа	O	-	[RESP_IEP_CorrAccLock]	Предзаполненное поле
2	Общие сведения	Статус заявки	O	-	[Исполнено] [Отклонено]	-
3		Комментарии	H	-	Текстовое поле	-

ПРИЛОЖЕНИЕ 27. ФОРМА ПРЕДСТАВЛЕНИЯ ДАННЫХ NTF_IEP_PUBLICATION – ФОРМА ПРЕДСТАВЛЕНИЯ УЧАСТНИКАМИ ИНФОРМАЦИОННОГО ОБМЕНА СВЕДЕНИЙ О ПЛАНИРУЕМЫХ МЕРОПРИЯТИЯХ ПО РАСКРЫТИЮ ИНФОРМАЦИИ О ВЫЯВЛЕННЫХ ИНЦИДЕНТАХ ЗАЩИТЫ ИНФОРМАЦИИ ИЛИ ИНЦИДЕНТАХ ОПЕРАЦИОННОЙ НАДЕЖНОСТИ

Порядковый номер	Категория элемента данных	Описание АСОИ UI	Обязательность полей	Условие обязательности	Правило заполнения	Примечание
1	Тип уведомления	Тип уведомления	O	-	[NTF_IEP_Publication]	Предзаполненное поле
2	Общие сведения	Наименование мероприятия	O	-	Текстовое поле	-
3		Дата мероприятия	O	-	Дата и время в формате: dd.mm.yyyy hh:mm	[UTC +03:00]
4		Описание	O	-	Текстовое поле	-
5		Организация	O	-	Текстовое поле	-
6	Контактное лицо	Фамилия	O	-	Текстовое поле	-
7		Имя	O	-	Текстовое поле	-
8		Отчество	H	-	Текстовое поле	-
9		Должность	O	-	Текстовое поле	-
10		e-mail-адрес	O	-	В соответствии с RFC 822	-
11		Городской телефон	O	-	В соответствии с международной системой и планом нумерации	-
12		Мобильный телефон	O	-	В соответствии с международной системой и планом нумерации	-
13	Мероприятие	Тип мероприятия	O	-	Текстовое поле	-
14		Текст мероприятия	O	-	Текстовое поле или файл	-

ПРИЛОЖЕНИЕ 28. ДОПОЛНИТЕЛЬНЫЕ КЛАССИФИКАТОРЫ, ИСПОЛЬЗУЕМЫЕ В НАСТОЯЩЕМ СТАНДАРТЕ

Наименование классификатора	Описание классификатора
Критерии легитимности операции без согласия	Признаки осуществления перевода денежных средств без согласия клиента, установленные Банком России
Источники риска	Классификатор событий риска реализации информационных угроз в разрезе источников риска в соответствии с ГОСТ Р 57580.3-2022
Типы объектов и субъектов	Классификатор источников риска в разрезе направлений типов атакуемых объектов в соответствии с ГОСТ Р 57580.3-2022
Технологические участки	Классификатор технологических участков в соответствии с нормативными актами Банка России

КЛАССИФИКАТОР «КРИТЕРИИ ЛЕГИТИМНОСТИ ОПЕРАЦИИ БЕЗ СОГЛАСИЯ»

Поле формы представления данных	Код критерия легитимности	Критерий легитимности
Критерии легитимности операции без согласия, характеризующие плательщика	[Statement]	Наличие заявления плательщика о несогласии с операцией
	[Atypical device]	Несоответствие устройства, с использованием которого осуществляется операция, или параметров устройства типичным для операций плательщика
	[Atypical actions]	Несоответствие действий, предшествующих операции, типичным (снятие с вклада, множественное получение средств от разных плательщиков, смена номера телефона, на который приходит OTP и т. д.)
	[Atypical session]	Несоответствие поведения в рамках сессии типичному (начало сессии без окончания предыдущей, запрос нескольких одноразовых паролей, множественные неуспешные попытки OTP и т. д.)
	[Robotization]	Выявление автоматизированных действий при формировании платежа
	[Absence]	Отсутствие у плательщика других финансовых продуктов (кредитные продукты, инвестиционные продукты и т. д.)
	[Mass registration]	Массовая регистрация / открытие платежных инструментов (карт, счетов)
	[Spoof of payment]	Признаки подмены реквизитов на стороне плательщика
	[Questionable source]	Признаки получения реквизитов получателя из ненадежного источника
	[Remote control]	Признаки наличия удаленного управления на устройстве плательщика
	[SIM replacement]	Признаки замены сим-карты клиента
	[Confirmed transactions]	Осуществление плательщиком ранее операций данному получателю, которые не были оспорены
	[Subscription]	Наличие у плательщика периодических платежей (подписки) на данного получателя, которые не были оспорены
	[Virus]	Наличие признаков воздействия вредоносного программного обеспечения на устройстве клиента
	[Change login/password]	Повторная регистрация или восстановление доступа в ДБО, смена логина/пароля для доступа
	[Tokenization]	Привязка, токенизация платежных инструментов (карт) на нетипичное устройство или на множество устройств
	[Retiree]	Является престарелым лицом или пенсионером
	[Anonymous]	Признаки использования плательщиком анонимизированных каналов связи, публичных VPN и proxy, облачных и выделенных серверов
	[Mass Retail]	Наличие большого количества операций покупок, нетипичных для клиента

Поле формы представления данных	Код критерия легитимности	Критерий легитимности
Критерии легитимности операции без согласия, характеризующие получателя средств	[Statement]	Наличие заявлений о несогласии с операцией в адрес данного получателя
	[Geolocation]	Одновременная работа в ДБО с различных геолокаций
	[Excceeding device]	Использование для входа в ДБО различных устройств, количество которых превышает среднестатистическое
	[Absence]	Отсутствие у получателя других финансовых продуктов (кредитные продукты, инвестиционные продукты и т. д.)
	[Mass registration]	Массовая регистрация / открытие платежных инструментов (карт, счетов)
	[Cashing out]	Обналичивание денежных средств при отсутствии других операций
	[Dropper]	Наличие большого количества операций по переводу денежных средств (C2C, B2B), при отсутствии других операций
	[Relationship]	Выявленная связь (административная, финансовая, техническая и т. д.) с лицами, внесенными в базу данных о случаях и попытках осуществления перевода денежных средств без согласия клиента
	[Absence transaction]	Отсутствие в профиле клиента операций хозяйственной деятельности
	[Anonymous]	Признаки использования получателем анонимизированных каналов связи, публичных VPN и proxy, облачных и выделенных серверов
	[Figurehead]	Признаки номинального руководства организацией
	[Titular owner]	Признаки номинального владельца платежным инструментом (картой, счетом)
	[Complaints]	Наличие жалоб на мошенничество в Интернете
	[Fraud/Sale]	Превышение соотношения фродовых и нефродовых операций по данному получателю (по сумме или по количеству) граничных значений, установленных кредитной организацией
	[Crypto]	Средство платежа получателя используется для операций с криптовалютой
	[Confirmed transactions]	Поступление ранее денежных средств от данного плательщика, которые не были оспорены
	[Wage]	Наличие зарплатного проекта
	[Technological account]	Счет получателя средств является технологическим счетом
	[Subscription]	Наличие периодических платежей (подписки) на данного получателя, которые не были оспорены
	[Government]	Является органом государственной власти
	[Financial institution]	Является организацией финансовой сферы (кредитные организации, субъекты Национальной платежной системы, некредитные финансовые организации)
	[GKH]	Является платежным агентом в сфере ЖКХ
	[Retail]	Является крупной организацией, занимающейся розничной торговлей
	[Vendor]	Является крупной организацией – поставщиком товаров или услуг
	[Mediator]	Является промежуточным получателем операции (например, сервис P2P-переводов)
	[Charity]	Является благотворительной организацией
Критерии легитимности операции без согласия, характеризующие операцию	[Atypical parametres]	Несоответствие параметров операции типичным операциям плательщика (сумма операции, периодичность операций, получатель денежных средств и т. д.)
	[Atypical conditions]	Несоответствие условий операции типичным для плательщика (геолокация плательщика, время суток осуществления операций и т. д.)
	[Atypical actions]	Несоответствие действий, предшествующих операции, типичным (снятие с вклада, множественное получение средств от разных плательщиков, смена номера телефона, на который приходит OTP и т. д.)
	[Atypical device]	Несоответствие устройства, с использованием которого осуществляется операция, или параметров устройства типичным для операций плательщика
	[Mass Retail]	Большое количество операций покупок за короткий промежуток времени нетипичных для клиента
	[Credit after new auth]	Оформление предодобренного кредитного продукта сразу после восстановления доступа в ДБО, смены логина/пароля, номера телефона OTP
	[Dispute]	Операция оспаривается в рамках претензионного цикла МПС или неполученного товара/услуги

КЛАССИФИКАТОР «ИСТОЧНИКИ РИСКА»

Код источника риска	Наименование источника риска	Дополнительная классификация событий риска реализации информационных угроз
[defectOfProcess]	Недостатки процессов	В целях дополнительной классификации событий риска реализации информационных угроз финансовая организация к категории «недостатки процессов» относит: – недостатки процессов применения технологических мер защиты информации, обрабатываемой в рамках технологических операций при выполнении бизнес- и технологических процессов; – недостатки процессов применения прикладного программного обеспечения автоматизированных систем и приложений, соответствующих требованиям к обеспечению защиты информации [8–10]; – недостатки процессов планирования, реализации, контроля и совершенствования процессов обеспечения операционной надежности и защиты информации; – недостатки других внутренних процессов, связанных с обеспечением операционной надежности и защиты информации финансовой организации
[actionOfStaff]	Действия персонала и других связанных с финансовой организацией лиц	В целях дополнительной классификации событий риска реализации информационных угроз финансовая организация к категории «действия персонала и других связанных с финансовой организацией лиц» относит реализацию несанкционированного доступа работников финансовой организации или третьих лиц, обладающих полномочиями доступа к объектам информатизации инфраструктурного уровня финансовой организации (действия внутреннего нарушителя)
[failureOfIT]	Сбои объектов информатизации (отказы и (или) нарушения функционирования применяемых финансовой организацией объектов информатизации и (или) несоответствие их функциональных возможностей и характеристик потребностям финансовой организации)	В целях дополнительной классификации событий риска реализации информационных угроз финансовая организация к категории «сбои объектов информатизации» относит сбои и отказы в работе объектов информатизации в результате реализации информационных угроз
[externalFactor]	Внешние факторы	В целях дополнительной классификации событий риска реализации информационных угроз финансовая организация к категории «внешние факторы» относит реализацию компьютерных атак или несанкционированного доступа лиц, не обладающих полномочиями доступа к объектам информатизации инфраструктурного уровня финансовой организации (действия внешнего нарушителя), в том числе с целью: – блокирования штатного функционирования бизнес- и технологических процессов финансовой организации; – хищения, искажения, удаления информации конфиденциального характера (включая персональные данные)

КЛАССИФИКАТОР «ТИПЫ ОБЪЕКТОВ И СУБЪЕКТОВ»

Код уровня объекта или субъекта	**Уровень объекта или субъекта**	**Код типа объекта или субъекта**	**Тип объекта или субъекта**
[Infrastructure]	Инфраструктурный уровень объектов информатизации (системный уровень информационной инфраструктуры)	[Hardware]	Аппаратное обеспечение
		[Network hardware]	Сетевое оборудование
		[Network applications and services]	Сетевые приложения и сервисы
		[Server virtualization components, software infrastructure services]	Серверные компоненты виртуализации, программные инфраструктурные сервисы
		[Operating systems, database management systems, application servers]	Операционные системы, системы управления базами данных, сервера приложений
[Application level to perform tech processes]	Прикладной уровень объектов информатизации (уровень автоматизированных систем и приложений), используемых для выполнения бизнес- и технологических процессов финансовой организации при оказании финансовых (банковских) и (или) информационных услуг	[System of remote banking]	Система дистанционного банковского обслуживания
		[System for processing transactions made using payment cards]	Система обработки транзакций, осуществляемых с использованием платежных карт
		[Information resource of the Internet]	Информационный ресурс сети Интернет
		[Automated banking system]	Автоматизированная банковская система
		[Post-transaction service system made using payment cards]	Система посттранзакционного обслуживания операций, осуществляемых с использованием платежных карт
		[Automated systems]	Автоматизированные системы, используемые работниками финансовой организации
[Application level used by the client]	Прикладной уровень объектов информатизации (уровень автоматизированных систем и приложений), используемых клиентом финансовой организации при получении финансовых услуг	[Mobile application]	Мобильное приложение
		[File server]	Файловый сервер
		[System of remote banking]	Система дистанционного банковского обслуживания
		[Email server]	Сервер электронной почты
		[Automated system]	Автоматизированная система, используемая работниками клиента финансовой организации
[Other object]	Другие атакуемые объекты	[Other system]	Другие системы, используемые финансовой организацией
[Subject]	Атакуемые субъекты	[Employee]	Работники финансовой организации
		[Client]	Клиенты финансовой организации
		[Partner]	Партнеры, контрагенты, подрядчики и т. д. финансовой организации

КЛАССИФИКАТОР «ТЕХНОЛОГИЧЕСКИЕ УЧАСТКИ»

Код технологического участка	Наименование технологического участка
[ИАА]	Идентификация, аутентификация и авторизация клиентов при совершении действий в целях осуществления банковских операций/финансовых операций или обработки, хранения и передачи защищаемой информации
[ФПП]	Формирование (подготовка), передача и прием электронных сообщений
[УП]	Удостоверение права клиентов распоряжаться денежными средствами, ценными бумагами или иным имуществом или на совершение действий с защищаемой информацией
[ОУ]	Осуществление банковской операции/финансовой операции или действий в целях обработки, хранения и передачи защищаемой информации, учет результатов их осуществления
[ХИ]	Хранение/учет электронных сообщений, информации об осуществленных банковских/финансовых операциях или действиях с защищаемой информацией, результатов осуществления действий в целях обработки, хранения и передачи защищаемой информации
[СборБО_ЕБС] [СборБО_КБС]	Для ЕБС: сбор биометрических персональных данных физических лиц и передача собранных биометрических персональных данных физических лиц между структурными подразделениями банка, мобильными (переносными) устройствами вычислительной техники (планшетами), платежными терминалами, банкоматами. Для КБС: сбор биометрических персональных данных физических лиц финансовыми организациям для целей передачи в информационные системы организаций финансового рынка и передачи собранных биометрических персональных данных физических лиц между структурными подразделениями банка, мобильными (переносными) устройствами вычислительной техники (планшетами), платежными терминалами, банкоматами
[ОбработкаБО_ЕБС] [ОбработкаБО_КБС]	Для ЕБС: обработка собранных биометрических персональных данных физических лиц с целью передачи в ЕБС с использованием СМЭВ. Для КБС: обработка биометрических персональных данных физических лиц финансовыми организациям для их размещения (обновления) в информационных системах организаций финансового рынка
[ПередачаБО_ЕБС]	Для ЕСБ: передача биометрических персональных данных физических лиц в ЕБС с использованием СМЭВ
[УИА_ЕБС] [УИА_КБС]	Для ЕСБ: удаленная идентификация или удаленная аутентификация клиента – физического лица. Для КБС: автоматизированная передача биометрических персональных данных физических лиц в информационные системы организации финансового рынка и их обработки на устройстве клиента – физического лица в целях идентификации физического лица без его личного присутствия с использованием биометрических персональных данных (далее – удаленная идентификация) и (или) аутентификации физического лица без его личного присутствия с использованием биометрических персональных данных (далее – удаленная аутентификация) физического лица
[ПроверкаУИА_ЕБС]	Для ЕБС: проверка результатов удаленной идентификации или удаленной аутентификации клиента – физического лица в ЕСИА и ЕБС
[ВзаимодействиеУИА_ЕБС]	Для ЕБС: взаимодействие банка с ЕСИА и ЕБС
[ПередачаБДБО_ЕБС]	Для ЕБС: передача собранных биометрических персональных данных между осуществляющими обработку биометрических персональных данных информационными системами организаций финансового рынка и ЕБС в случае, указанном в части 18.23 статьи 14.1 Федерального закона № 149-ФЗ
[ОбработкаУИА_КБС]	Для КБС: обработка биометрических персональных данных (за исключением сбора), а также информации о степени соответствия в информационных системах организаций финансового рынка в целях проведения идентификации и (или) аутентификации в случае выполнения условий, установленных в частях 18.18 и 18.20 статьи 14.1 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – Федеральный закон № 149-ФЗ)
[ПередачаУИА_КБС]	Для КБС: передача биометрических персональных данных физических лиц, а также информации о степени их соответствия в информационные системы организаций финансового рынка в целях проведения идентификации и (или) аутентификации с использованием стационарных технических средств структурных подразделений финансовых организаций, мобильных (переносных) устройств вычислительной техники (планшетов), принадлежащих финансовым организациям, платежных терминалов, банкоматов
[ДелегированиеУИА_КБС]	Для КБС: взаимодействие финансовых организаций, иных организаций, индивидуальных предпринимателей с информационными системами организаций финансового рынка в целях аутентификации физического лица

БИБЛИОГРАФИЯ

[1]	Федеральный закон от 10 июля 2002 года N° 86-ФЗ «О Центральном банке Российской Федерации (Банке России)»
[2]	Федеральный закон от 26 июля 2017 года N° 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»
[3]	Федеральный закон от 27 июня 2011 года N° 161-ФЗ «О национальной платежной системе»
[4]	Федеральный закон от 20 июля 2020 года N° 211-ФЗ «О совершении финансовых сделок с использованием финансовой платформы»
[5]	Положение Банка России от 17 апреля 2019 года N° 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента»
[6]	Положение Банка России от 4 июня 2020 года N° 719-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»
[7]	Положение Банка России от 20 апреля 2021 года N° 757-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций»
[8]	Положение Банка России от 25 июля 2022 года N° 802-П «О требованиях к защите информации в платежной системе Банка России»
[9]	Положение Банка России от 12 января 2022 года N° 787-П «Об обязательных для кредитных организаций требованиях к операционной надежности при осуществлении банковской деятельности в целях обеспечения непрерывности оказания банковских услуг»
[10]	Положение Банка России от 15 ноября 2021 года N° 779-П «Об установлении обязательных для некредитных финансовых организаций требований к операционной надежности при осуществлении видов деятельности, предусмотренных частью первой статьи 76.1 Федерального закона от 10 июля 2002 года N 86-ФЗ «О Центральном банке Российской Федерации (Банке России)», в целях обеспечения непрерывности оказания финансовых услуг (за исключением банковских услуг)»
[11]	Положения Банка России от 08.04.2020 N° 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе»
[12]	Национальный стандарт Российской Федерации ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер»
[13]	Национальный стандарт Российской Федерации ГОСТ Р 57580.3-2022 «Безопасность финансовых (банковских) операций. Управление риском реализации информационных угроз и обеспечение операционной надежности. Общие положения»